# LEI DE SYLVESTER FRACA

*HELENA MARIA LÜDKE*

UNICAMP

**UNIVERSIDADE ESTADUAL DE CAMPINAS**

**INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E CIÊNCIA DA COMPUTAÇÃO**

CAMPINAS - SÃO PAULO
BRASIL

LEI DE SYLVESTER FRACA

Este exemplar corresponde à redação final da Tese devidamente corrigida defendida pela Srta. Helena Maria Lüdke e aprovada pela Comissão Julgadora.

Campinas, 10 de [illegible] 1985.

Prof. Dr. ANTONIO JOSÉ ENGLER
Orientador

Dissertação apresentada no Instituto de Matemática, Estatística e Ciência da Computação, UNICAMP, como requisito parcial para a obtenção do Título de Mestre em Matemática.

Janeiro - 1985

À minha irmã e aos
meus pais

AGRADEÇO

Ao Prof. Dr. Antônio José Engler, pela orientação e pela atenção e incentivos recebidos.

À Iveli, pela confiança e acompanhamento do processo de solicitação de licença para qualificação profissional do cargo no Magistério Público do Estado do Rio Grande do Sul.

À Dorly e à Solange, pela oportunidade da convivência.

Ao Ary, pelo coleguismo e amizade.

À CAPES, pela ajuda financeira.

À Universidade de Caxias do Sul, pela inclusão no Programa Institucional de Capacitação de Docentes.

*Helena Maria Lüdke*

ÍNDICE

# INTRODUÇÃO

Determinar condições que assegurem a isotropia de formas quadráticas é, em geral, um problema não muito fácil. Relacionado com essa questão surge, de modo natural, em corpos formalmente reais um outro aspecto: a isotropia fraca de formas quadráticas. Se $\rho$ é uma forma quadrática sobre um corpo $F$ pode-se perguntar se existe um número natural $m$ tal que $m\rho$ seja isotrópica. Conforme exista ou não tal $m$, $\rho$ é dita fracamente isotrópica ou fortemente anisotrópica. A noção de isotropia fraca de formas quadráticas foi introduzida por Prestel ([P](1973) e [P](1975)). Mais tarde foi estendida por Becker a formas de grau 2n. O presente trabalho trata desse tipo de isotropia. A maioria dos resultados apresentados são baseados nos trabalhos de Prestel.

No Capítulo I são caracterizados os corpos formalmente reais nos quais uma forma quadrática é fracamente isotrópica se e somente se ela é isotrópica em todos os fechos reais. Trata-se de uma propriedade de natureza "local-global" denominada Lei de Sylvester Fraca e denotada por L.S.F.. A caracterização é obtida (Teorema 1.32) através do estudo das formas quadráticas em conexão com uma generalização de cones positivos e ordens de um corpo: os q-cones e as q-ordens. O capítulo inclui noções e resultados básicos da teoria de Artin-Schreier sobre corpos formalmente reais que são usados com certa regularidade. Um estudo e demonstrações mais detalhadas sobre corpos formalmente reais podem ser encontrados em [P](1975), [J] ou [R].

A classe dos corpos que satisfazem a L.S.F. é exatamente a classe dos corpos nos quais toda q-ordem é uma ordem e coincide portanto (conforme [P] (1975) Teorema 9.1) com a classe dos corpos cujo espaço das ordens satisfaz a "Propriedade de Aproximação Forte" ("Strong Approximation Property").

No Capítulo II os corpos que satisfazem a L.S.F. são caracterizados através de suas valorizações reais (valorizações com corpo de resíduos formalmente real). Os principais resultados são: o Teorema 2.24 que mostra um processo de construção de uma q-ordem do corpo a partir de uma q-ordem no corpo de resíduos; o Teorema 2.27 que dá a caracterização citada; e o Teorema 2.33 sobre a Hereditariedade da L.S.F.(que é uma contribuição original do trabalho). Os dois primeiros são resultados de Prestel e o terceiro surge ao analisar o "going up" e o "going down" da L.S.F.. No §2 desse capítulo o resultado mais importante é o Teorema 2.45 que caracteriza os corpos henselianos com aproximação forte. No §3 são apresentados exemplos de corpos que satisfazem a L.S.F. e com q-ordem própria.

De maneira semelhante ao clássico Princípio Local Global de Hasse-Minkowski que permite reduzir a questão da isotropia à respectiva questão nos completamentos relativos às topologias induzidas por valorizações, os Teoremas 3.2 e 3.8 do capítulo III mostram que a isotropia fraca de uma forma quadrática pode ser analisada estudando a correspondente questão nos completamentos relativos à valorizações reais e ordens arquimedianas ou à correspondente questão nas henselizações relativas às valorizações reais e nos fechos reais relativos às ordens arquimedianas. São teoremas devidos a Prestel. O Teorema 3.8 também foi provado independentemente por Bröcker ([Br]).

Finalmente, no Capítulo IV é analisada a isotropia fraca em corpos de funções algébricas.

É sabido que a questão da isotropia de formas quadráticas pode ser analisada estudando o anel de Witt do corpo. Algumas vezes são feitas referencias a esse anel. A teoria à respeito pode ser encontrada em [L] , assim como toda a teoria sobre formas quadráticas da qual é feito uso e sobre a qual são introduzidas apenas noções essenciais.

Deve-se salientar que todos os corpos considerados possuem característica diferente de 2. E que, como pelo Teorema 1.27 o estudo de isotropia fraca só faz sentido em corpos formalmente reais, está se supondo, nos teoremas referentes à essa noção, que os corpos são formalmente reais.

# CAPÍTULO I

# LEI DE SYLVESTER FRACA

O primeiro parágrafo desse capítulo apresenta noções e resultados básicos da teoria de Artin-Schreier sobre corpos formalmente reais; no §2 é introduzido o conceito de q-ordens ; no §3 é introduzido o conceito de isotropia fraca de formas quadráticas e, por último, no §4 é estabelecida a conexão de q-ordens com formas quadráticas.

## §1 - CORPOS FORMALMENTE REAIS

Seja $F$ um corpo. Uma ordem de $F$ é um subconjunto $P \subset F$ que satisfaz:

(1.1) i) $P+P \subset P$ ii) $P.P \subset P$ iii) $P \cup -P = F$ iv) $-1 \notin P$.

Toda ordem satisfaz, além disso, $P \cap -P = \{0\}$.

Os elementos de $P-\{0\}$ são chamados *elementos positivos* de $F$ e $P$ é chamado *cone positivo* de $F$.

Uma ordem $P$ define em $F$ uma relação binária $\leq$ dada por:

$$a \leq b \leftrightarrow b-a \in P$$

e que satisfaz:

(1.2) (i) $\leq$ é uma relação de ordem total em $F$, isto é, para quaisquer $a,b,c \in F$ vale:

1) $a \leq a$

2) $a \leq b$ e $b \leq a \Rightarrow a = b$

3) $a \leq b$ e $b \leq c \Rightarrow a \leq c$

4) $a \leq b$ ou $b \leq a$

(ii) $a < b \Rightarrow a + c \leq b + c$, para todo $a,b,c \in F$.

(iii) $0 \leq a$, $0 \leq b \Rightarrow 0 \leq ab$, para todo $a,b \in F$.

Reciprocamente, uma relação binária $\leq$ que satisfaz as condições de (1.2) determina em $F$ o conjunto $P = \{x \in F;\ x \geq 0\}$ que satisfaz as condições de (1.1). Nesse caso, $P$ é chamado *cone positivo de* $\leq$.

Desde que a correspondência citada é biunívoca as ordens de $F$ são denotadas indistintamente por $\leq$ ou $P$.

Um corpo com uma ordem é um *corpo ordenado*. Em geral, um corpo $F$ pode admitir diferentes ordens. Indicaremos por $(F,P)$ ou $(F,\leq)$ o corpo $F$ com a sua estrutura de corpo ordenado induzida pela ordem $P$ ou $\leq$.

Denotaremos por $\Sigma F^2$ o conjunto dos elementos de $F$ que são somas de quadrados, isto é, $\Sigma F^2 = \{x_1^2 + \ldots + x_n^2;\ x_i \in F\}$.

Se $-1 \in \Sigma F^2$ então $\Sigma F^2 = F$, pois, para todo $a \in F$ temos $a = (\frac{a+1}{2})^2 - (\frac{a-1}{2})^2$. Corpos nos quais $-1$ não é soma de quadrados são chamados *formalmente reais*.

No Teorema 1.4 mostraremos que os corpos formalmente reais são exatamente os corpos ordenáveis, isto é, os corpos para os quais o conjunto dos cones positivos não é vazio. Para isso, vamos estabelecer, na linguagem de cones, o conceito de pré-ordem.

1.3 - DEFINIÇÃO: Seja $F$ um corpo. Uma *pré-ordem* (ou *pré-cone positivo*) de $F$ é um conjunto $P \subset F$ tal que:

$$P+P \subset P \qquad P.P \subset P \qquad F^2 \subset P \qquad -1 \notin P.$$

É imediato que: i) $\Sigma F^2 \subset P$ para todo pré-cone positivo $P$ de $F$; ii) $\Sigma F^2$ é fechado aditivamente e iii) $\Sigma F^2$ é um subgrupo multiplicativo de $F^{\bullet}$.

1.4 - TEOREMA: *Seja $F$ um corpo. $F$ é ordenável se e somente se $F$ é formalmente real.*

DEMONSTRAÇÃO: Se $P$ é uma ordem de $F$ então $F = P \cup -P$ implica que $F^2 \subset P$ e, como $1 \in P$ e $P \cap -P = \{0\}$, temos que $-1 \notin \Sigma F^2$.

Reciprocamente, se considerarmos que $-1 \notin \Sigma F^2$ então o conjunto $\Sigma F^2$ é uma pré-ordem de $F$. Pelo Lema de Zorn, o conjunto das pré-ordens de $F$ que estendem $\Sigma F^2$ possui um elemento maximal $P$. Suponhamos que $P \cup -P \neq F$ e seja $a \in F \setminus (P \cup -P)$. Então, $P + Pa$ é uma pré-ordem de $F$ tal que $P \subsetneqq P + Pa$, contrariando a maximalidade de $P$. Logo, $P \cup -P = F$ e $P$ é uma ordem de $F$. ∎

Usando raciocínio semelhante à demonstração do Teorema 1.4 mostra-se que os elementos totalmente positivos de $F$ (= positivos em todas as ordens) são as somas de quadrados de $F$, isto é, $\Sigma F^2 = \cap P$, onde $P$ percorre o conjunto de todos os cones de $F$.

1.5 - TEOREMA (Artin-Schreier): *Seja $F$ um corpo e $a \in F$. Então, $a \in F$ é totalmente positivo se e somente se $a \in \Sigma F^2$.*

DEMONSTRAÇÃO: Como $\Sigma F^2 \subset P$ para todo cone positivo $P$, basta mostrar que se $a \in \cap P$ então $a \in \Sigma F^2$. Se $a \notin \Sigma F^2$ então $\Sigma F^2 - a\,\Sigma F^2$ é uma pré-ordem de $F$ e, portanto, se estende a uma ordem $P_0$ de $F$. Como $-a \in P_0$ e $P_0 \cap -P_0 = \{0\}$, temos uma contradição com a escolha de $a$. ■

Utilizando esse resultado caracteriza-se facilmente corpos com uma única ordem.

1.6 - PROPOSIÇÃO: *Seja $F$ um corpo. $\Sigma F^2$ é uma ordem de $F$ se e somente se $F$ possui uma única ordem.*

DEMONSTRAÇÃO: Seja $P$ a única ordem de $F$. Se existe $x \in P$ tal que $x \notin \Sigma F^2$ temos $-x \in \Sigma F^2 \subset P$, o que é uma contradição. Logo $P = \Sigma F^2$.

Reciprocamente, se $x \notin \Sigma F^2$ e $-x \notin \Sigma F^2$ existem ordens $P_1$ e $P_2$ de $F$ tais que $x \notin P_1$ e $-x \notin P_2$. Mas, então, $-x \in P_1$ e $x \in P_2$, isto é, $P_1 \neq P_2$, o que é uma contradição. ■

Exemplos de corpos com uma única ordem são: o corpo $\mathbb{R}$ dos números reais e o corpo $\mathbb{Q}$ dos números racionais. A única ordem de $\mathbb{R}$ é $\mathbb{R}^2$ é a única ordem de $\mathbb{Q}$ é $\Sigma\mathbb{Q}^2 = \mathbb{R}^2 \cap \mathbb{Q}$.

O seguinte teorema estabelece mais caracterizações de corpos formalmente reais, facilmente demonstráveis.

1.7 - TEOREMA: *Seja* F *um corpo são equivalentes:*

(i) F *é ordenável*

(ii) $-1 \notin \Sigma F^2$

(iii) $\sum_{i=1}^{n} a_i^2 = 0 \Rightarrow a_i = 0$ *para todo* $1 \leq i \leq n$.

(iv) $F \neq \Sigma F^2$

Por (iii) a característica de um corpo formalmente real é zero. Assim, se F é um corpo formalmente real então, o corpo dos números racionais é canonicamente isomorfo a um subcorpo de F e podemos considerar $\mathbb{Q} \subset F$.

Dado um corpo ordenado (F,P) e uma extensão $F_1$ de F uma questão importante é saber se existe em $F_1$ uma ordem $P_1$ tal que $P_1 \cap F = P$. Se isso ocorre, então dizemos que P *pode ser estendida a* F e que $P_1$ *estende* P. $(F_1,P_1)$ é chamada *extensão ordenada* de (F,P).

Um corpo F com uma ordem P é chamado *ordenado maximal* se para toda extensão ordenada $(F_1,P_1)$ de (F,P), F é algebricamente fechado em $F_1$.

Na teoria dos corpos ordenados os corpos ordenados maximais são particularmente interessantes. Na Proposição a seguir, damos suas possíveis caracterizações:

1.8 - PROPOSIÇÃO: *Seja* (F,P) *um corpo ordenado. São equivalentes:*

1) $(F,P)$ *é ordenado maximal.*

2) $P = F^2$ *e todo polinômio de grau ímpar com coeficientes em* $F$ *possui raiz em* $F$.

3) $F(\sqrt{-1})$ *é algebricamente fechado.*

DEMONSTRAÇÃO:

1) $\Rightarrow$ 2) Seja $f \in F[x]$ um polinômio de grau ímpar ou $f = x^2 - a$ com $a \in P$. Seja $b$ uma raiz de $f$. Contrói-se de maneira natural uma ordem $P'$ de $F(b)$ que estende $P$. Logo $F(b)=F$.

2) $\Rightarrow$ 3) Com o auxílio da teoria de Galois demonstra-se que os únicos polinômios irredutíveis com coeficientes em $F$ de grau maior que 1 são do tipo $ax^2 + bx + c$ com $b^2 - 4ac \notin P$. Todos esses polinômios possuem suas raízes em $F(\sqrt{-1})$. Logo $F(\sqrt{-1})$ é algebricamente fechado.

3) $\Rightarrow$ 1) É imediato. ■

Outra noção importante da teoria de Artin-Schreier é a noção de corpo real fechado e a de fecho real. É a idéia análoga à de corpo algebricamente fechado e de fecho algébrico.

Um corpo se diz *real fechado* se é formalmente real mas não possui extensão algébrica própria que seja formalmente real.

Se $P$ for uma ordem de um corpo real fechado $F$ e $a \in P^{\bullet}$, então $P$ se estende a $F(\sqrt{a})$. Mas então, $F(\sqrt{a}) = F$, pois, $F(\sqrt{a})$ é uma extensão algébrica de $F$. Assim, $a \in F^2$ e $F^2$ é a única ordem de $F$. Do mesmo modo, por 1.8(2), se $(F,P)$ é ordenado maximal então, $F$ possui uma única ordem.

1.9 - PROPOSIÇÃO: *Seja* $F$ *um corpo formalmente real.* $F$ *é real* *fechado se e somente se* $F$ *é ordenado maximal.*

DEMONSTRAÇÃO: ( $\Rightarrow$ ) É imediato

( $\Leftarrow$ ) Desde que $F$ possui uma única ordem $P$, toda ordem $P_1$ de qualquer extensão $F_1$ de $F$, formalmente real, estende a ordem $P$ de $F$ e, portanto, se $F_1$ é extensão algébrica de $F$, então $F_1 = F$. ∎

Para todo corpo $R$ real fechado vale o seguinte:

(1.10) i) Se $f \in R[x]$ então $f$ se decompõe em fatores irredutíveis do tipo $x - a$ ou $(x-a)^2 + b^2$ para $a,b \in R$.

ii) Se $f \in R[x]$ e existem $a,b \in R$ tais que $a < b$ e $f(a) < 0 < f(b)$ então existe $c \in R$ tal que $a < c < b$ e $f(c) = 0$.

iii) Se $f = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in R[x]$ então, para todo $\alpha \in R$ tal que $f(\alpha) = 0$, $|\alpha| < \mu = \text{máx}\ \{1, |a_0| + \ldots + |a_{n-1}|\}$

iv) Se $F$ é um subcorpo de $R$ então o fecho algébrico de $F$ em $R$ é um corpo real fechado.

v) $|\dot{R}/\dot{R}^2| = 2$.

A todo corpo ordenado $(F,P)$ pode ser associada uma extensão $R$ com as propriedades:

(1.11) i) $R$ é uma extensão algébrica de $F$.

ii) $R$ é um corpo real fechado cuja única ordem estende $P$.

A existência de um corpo $R$ com as propriedades de (1.11) é garantida pela aplicação do Lema de Zorn e a unicidade, a menos de F-isomorfismos, pode ser demonstrada utilizando o teorema de zeros de Sturm que dá os zeros de uma função polinomial em um intervalo de R com base na observação da troca de sinais de uma família de polinômios.

Devido a unicidade, salvo F-isomorfismos, o corpo R com as propriedades i) e ii) de (1.11) é chamado *o fecho real de* (F,P).

1.12 - TEOREMA: *Todo corpo ordenado* (F,P) *possui, a menos de F-isomorfismos, um único fecho real.*

## §2 - q-ORDENS

O conceito de q-ordem é uma generalização do conceito de ordem.

1.13 - DEFINIÇÃO: Seja F um corpo. Uma *q-ordem* de F é um subconjunto $P \subset F$ tal que:

i) $P+P \subset P$ ii) $F^2P \subset P$ e $1 \in P$ iii) $P \cap -P = \{0\}$

iv) $P \cup -P = F$.

Se P é uma q-ordem de F diremos que (F,P) é um *corpo q-ordenado* e P é um *q-cone de* F.

De maneira análoga ao que ocorre com as ordens de um corpo F, uma q-ordem P de F define em F uma relação binária $\leq$ dada por:

$$a \leq b \leftrightarrow b - a \in P$$

que satisfaz

1) $\leq$ é uma relação de ordem total em F.

2) $a \leq b \Rightarrow a + c \leq b + c$, para quaisquer $a,b,c \in F$.

3) $0 \leq a \Rightarrow 0 \leq ab^2$, para quaisquer $a,b \in F$.

Reciprocamente, uma relação binária que satisfaz as condições 1), 2) e 3) determina em F o conjunto $P = \{x \in F; 0 \leq x\}$ que satisfaz as condições i) a iv). Nesse caso P é chamado *q-cone* de $\leq$.

Desde que essa correspondência, assim como nas ordens, é biunívoca, podemos nos referir indistintamente a $\leq$ e P como q-ordens de F e a (F,P) e $(F,\leq)$ como *corpo q-ordenado*.

Substituindo 3) por $(0 \leq a$ e $0 \leq b) \Rightarrow 0 \leq ab$ a relação $\leq$ passa a ser uma ordem de F. Do mesmo modo, se em ii) tivermos $P \cdot P \subset P$ então P é um cone positivo de F.

É fácil perceber que todo q-cone contém $\Sigma F^2$ e que toda ordem é um q-ordem.

Uma q-ordem que não é ordem é dita *q-ordem própria*.

Exemplos de corpos que possuem q-ordens próprias são $\mathbb{Q}(x)$ e $\mathbb{R}(x,y)$, conforme ficará claro no Capítulo II.

Na proposição 1.14 demonstraremos propriedades sobre q-ordens que são usadas com frequência e que tornam claras as semelhanças e diferenças entre ordens e q-ordens. Serão utilizados os fatos já mencionados de que $\Sigma F^2$ é aditivamente fechado e $\Sigma F^2 - \{0\}$ é um subgrupo multiplicativo de $F^{\bullet}$.

1.14 - PROPOSIÇÃO: *Seja* $\leq$ *uma q-ordem de um corpo* F.*Então, para quaisquer* $x, y \in F$ *vale:*

i) $0 < x \Rightarrow 0 < \frac{1}{x}$

ii) $0 < x < y \Rightarrow yx^2 < xy^2$

iii) $0 < x < y \Rightarrow \frac{1}{y} < \frac{1}{x}$

iv) $0 < x < y,\ x \in \Sigma F^2 \Rightarrow x^2 < y^2$

v) $0 < x < y,\ y \in \Sigma F^2 \Rightarrow x^2 < y^2$

vi) $0 < x < 1 \Rightarrow x^2 < x$

vii) $1 < y \Rightarrow y < y^2$

DEMONSTRAÇÃO:

i) $0 < x \Rightarrow 0 < x(\frac{1}{x})^2 = \frac{1}{x}$

ii) $0 < x < y \Rightarrow 0 < x$ e $0 < y - x \Rightarrow 0 < \frac{1}{y-x} + \frac{1}{x} \Rightarrow$

$$\Rightarrow 0 < \frac{1}{\frac{1}{y-x} + \frac{1}{x}} y^2 = xy^2 - x^2y \Rightarrow x^2y < xy^2$$

iii) De ii) temos $0 < -x^2y + xy^2$, o que implica em

$0 < \frac{1}{(xy)^2}(-x^2y + xy^2) = \frac{1}{x} - \frac{1}{y}$. Logo $\frac{1}{y} < \frac{1}{x}$.

iv) $0 < x < y \Rightarrow yx^2 < xy^2 \Rightarrow 0 < xy^2 - yx^2 \Rightarrow 0 < (xy^2 - yx^2)\frac{1}{x}$

$= y^2 - yx \Rightarrow yx < y^2$. Da mesma forma $x < y \Rightarrow x^2 < xy$.

Logo $x^2 < y^2$.

v) A prova é análoga a iv).

vi) Basta fazer $y = 1$ em (ii).

vii) Basta fazer $x = 1$ em (ii). ■

Convém notar que:

1) Numa q-ordem $\leq$, se $0 \leq a$ e $0 \leq b$ não necessariamente $0 \leq ab$.

2) Uma q-ordem é uma ordem se e somente se $0 < a < b \Rightarrow$ $\Rightarrow a^2 < b^2$.

3) De vi) e vii) e usando demonstração por indução obtem-se:

$$0 < x < 1 < y \Rightarrow 0 < x^{n+1} < x^n < 1 < y^m < y^{m+1}$$

para quaisquer $x,y \in F$ e $m,n \in \mathbb{N} - \{0\}$.

4) Se $P$ é uma q-ordem de $F$ e $|x|$ é definido por $|x|=x$ quando $x \in P$ e $|x| = -x$ quando $x \in -P$ então, $|ab|=||a||b||$, mas não podemos afirmar que $|ab|= |a||b|$. Se $a \in \Sigma F^2$ então, $|ab| = a|b|$.

As ordens são classificadas em arquimedianas e não arquimedianas. Uma ordem $\leq$ é chamada arquimediana se para todo $a > 0$ existe $n \in \mathbb{N}$ tal que $n > a$.

Conforme o teorema de Ostrowski ([E] Teorema 2.10) sabemos que, se $F$ tem ordem arquimediana então, existe um isomorfismo ordenado de $F$ em $\mathbb{R}$. Definindo, de maneira análoga, q-ordem arquimediana, constataremos, pela Proposição 1.16 que para q-ordens vale um teorema análogo ao mencionado.

1.15 - DEFINIÇÃO: *Uma q-ordem $\leq$ é arquimediana se para todo $a \in F$ existe $n \in \mathbb{N}$ tal que $a < n$.*

1.16 - PROPOSIÇÃO: *Toda q-ordem arquimediana $\leq$ de um corpo F é uma ordem.*

DEMONSTRAÇÃO: Sejam $a, b \in F$ com $0 < a < b$. Então, $0 < 2a$ pois $2 \in \Sigma F^2$. Por 1.14(i), $0 < (2a)^{-1}$. Como $\leq$ é arquimediana, existe $n \in \mathbb{N}$ tal que $(2a)^{-1} < n$. Por 1.14(iii), $0 < \frac{1}{n} < 2a$. Seja $m \in \mathbb{N}$ o menor número natural tal que $m > n(b-a)$. Então, $m < n(b+a)$ pois, se ocorresse o contrário teríamos $n(b+a) - n(b-a) = 2an \leq 1$ e, como $n^{-1} \in \Sigma F^2$, $2a \leq \frac{1}{n}$. De $n(b-a) < m < n(b+a)$ temos então, novamente porque $n^{-1} \in \Sigma F^2$, que $b - a < \frac{m}{n} < b + a$. Por 1.14 (iv) e (v), $0 < (b-a)^2 < (\frac{m}{n})^2 < (b+a)^2$, pois $\frac{m}{n} \in \mathbb{Q}$ implica que $\frac{m}{n} \in \Sigma F^2$. Logo $0 < 4ab$, ou seja, $0 < ab$, pois $\frac{1}{4} \in \Sigma F^2$. ■

Assim, só há interesse em estudar q-ordens não arquimedianas.

Com a Proposição 1.16 é fácil constatar que um corpo de números não possui q-ordens próprias.

De fato:

Seja F um corpo de números algébricos. Basta mostrar que toda q-ordem de F é arquimediana. Sejam $a \in F$, $\leq$ uma q-ordem de F e $1 < a$. Então, pela Proposição 1.14 (vii), $1 < a < a^2$. Multiplicando por $a^2$ temos $a^2 < a^3 < a^4$. Continuando, sucessivamente, a multiplicar por $a^2$ obtemos $1 < a < a^2 < \ldots < a^m < a^{m+1} \ldots$. Assim qualquer que seja $m \in \mathbb{N}$, $\frac{1}{a^{m+1}} < 1$. Como a é algébrico sobre $Q$, existem $r_{n-1},\ldots,r_0 \in Q$ tais que $a^n + r_{n-1}a^{n-1}+\ldots+r_0 = 0$. Mas então, $a = -(r_{n-1}+\frac{r_{n-2}}{a}+\ldots+\frac{r_0}{a^{n-1}})$ e $a \leq \sum_{m=0}^{n-1} |r_{n-1-m}\cdot\frac{1}{a^m}| < \sum_{m=0}^{n-1}|r_m| \in Q$ e, portanto, existe $k \in \mathbb{N}$ tal que $a < k$. Logo, a q-ordem $\leq$ é arquimediana.

Analogamente à pré-cone define-se pré-q-cone:

1.17 - DEFINIÇÃO: Um conjunto $P \subset F$ é um *pré-q-cone* se satisfaz:

1) $P+P \subset P$

2) $F^2 . P \subset P$

3) $P \cap -P = \{0\}$

Convém notar que na Definição 1.17 nada é afirmado a respeito da unidade "1" de $F$.

Na Proposição 1.19 provaremos que dado um pré-q-cone $P$ existe um q-cone $P'$ tal que $P \subset P'$ ou $-P \subset P'$. Com esse objetivo enunciamos o seguinte lema que também será útil no §4 desse Capítulo.

1.18 - LEMA: *Sejam* $F$ *um corpo formalmente real,* $P$ *um pré-q-cone de* $F$ *e* $x \in F$ *tal que* $x \notin P$. *Existe um pré-q-cone* $P'$ *de* $F$ *tal que* $P \subset P'$ *e* $-x \in P'$.

PROVA: Seja $P' = P - x\Sigma F^2$. $P'$ satisfaz 1) e 2) de 1.17. Falta, então, mostrar que $P' \cap -P' = \{0\}$. Se $y \in P' \cap -P$ então $y = p - xs$ e $y = -(p_1 - xs_1)$ para $p,p_1 \in P$ e $s,s_1 \in \Sigma F^2$. Assim, $p - xs = -(p_1 - xs_1)$ e $(p+p_1) - x(s+s_1)=0$. Se $s+s_1 \neq 0$, então $x = (p+p_1)(s+s_1)^{-1} \in P$ dá uma contradição. Logo, $s+s_1 = 0$. Mas então, $p+p_1=0$ e, portanto, $p=-p_1 \in P \cap -P = \{0\}$, isto é, $p=p_1=0$. Como $F$ é formalmente real, por 1.7 (iii), $s=s_1=0$. Logo, $y = 0$ e $P'$ é um pré-q-cone com $P \subset P'$ e $-x \in P'$. ■

1.19 - PROPOSIÇÃO: *Sejam $F$ um corpo formalmente real e $P_0$ um pré-q-cone de $F$. Existe um conjunto $P \subset F$ tal que $P_0 \subset P$ e $P$ ou $-P$ é um q-cone de $F$.*

DEMONSTRAÇÃO: Pelo Lema de Zorn, o conjunto dos pré-q-cones tais que $P_0 \subset P$ possui elemento maximal. Seja $P$ esse pré-q-cone maximal. Se $x \notin P$, pelo Lema anterior, existe um pré-q-cone $P'$ tal que $P \subset P'$ e $-x \in P'$. Pela maximalidade de $P$ temos, então, $-x \in P$. Portanto, $P \cup -P = F$ e $P$ ou $-P$ é um q-cone. ■

1.20 - COROLÁRIO: *Seja $F$ um corpo formalmente real. $\Sigma F^2 = \cap P$ onde $P$ percorre o conjunto dos q-cones de $F$.*

DEMONSTRAÇÃO: Seja $a \in \cap P$. Suponhamos que $a \notin \Sigma F^2$. Então, como $\Sigma F^2$ é um pré-q-cone, pelo Lema 1.18 e Proposição 1.19, existe um q-cone $P$ tal que $\Sigma F^2 \subset P$ e $-a \in P$. Como $P \cap -P = \{0\}$, temos que $a \notin P$, contrariando a escolha de $a$. Por outro lado, para todo q-cone $P$ de $F$, $\Sigma F^2 \subset P$, isto é, $\Sigma F^2 \subset \cap P$. ■

1.21 - COROLÁRIO: *Seja $F$ um corpo. $F$ é formalmente real se e somente se $F$ admite uma q-ordem.*

DEMONSTRAÇÃO: ($\Rightarrow$) Desde que toda ordem é uma q-ordem, se $F$ é formalmente real então $F$ admite uma q-ordem.

($\Leftarrow$) Suponhamos que $F$ não é formalmente real. Então $-1 \in \in \Sigma F^2 = \cap P$ onde $P$ percorre o conjunto dos q-cones de $F$. Mas, então, $1 \in P$ e $-1 \in P$ para todo q-cone $P$ e, portanto, $1 \in \in P \cap -P = \{0\}$, o que é uma contradição. ∎

## §3 - ISOTROPIA FRACA DE FORMAS QUADRÁTICAS

Seja $F$ um corpo de característica diferente de 2.

Uma *forma quadrática* $\rho$ sobre $F$, de dimensão $n$, é um polinômio de $n$ variáveis com coeficientes em $F$, homogêneo e de grau 2, isto é:

$\rho = \sum_{1 \leq i,j \leq n} b_{ij} X_i X_j$ onde $b_{ij} \in F$, $X_i$ e $X_j$ são indeterminadas sobre $F$.

O estudo das formas quadráticas sobre um corpo pode ser reduzido às formas quadráticas do tipo $\rho(X_1, \ldots, X_n) = \sum_{i=1}^{n} a_i X_i^2$ com $a_i \neq 0$. Para estas, usaremos a notação $\rho = \langle a_1, \ldots, a_n \rangle$.

A *soma ortogonal* de duas formas quadráticas $\rho = \langle a_1, \ldots, a_n \rangle$ e $\rho_1 = \langle b_1, \ldots, b_m \rangle$ que representamos por $\rho \oplus \rho_1$ corresponde à forma $\langle a_1, \ldots, a_n, b_1, \ldots, b_m \rangle$ de dimensão $n + m$.

Se $m$ é um número natural, representamos a forma $\rho \oplus \ldots \oplus \rho$ ($m$ vezes) por $m\rho$.

O *produto tensorial* das formas $\rho$ e $\rho_1$ indicado por $\rho \otimes \rho_1$ corresponde à forma $\langle a_1 b_1, \ldots, a_1 b_m, \ldots, a_n b_1, \ldots, a_n b_m \rangle$

de dimensão n.

Um dos principais problemas na teoria de formas quadráticas é saber quando existe em F uma solução não trivial da equação $\sum_{i=1}^{n} a_i X_i^2 = 0$. Se existir uma solução não trivial a forma quadrática $<a_1,\ldots,a_n>$ é dita *isotrópica em* F. Se a única solução da equação for a trivial a forma $<a_1,\ldots,a_n>$ é dita *anisotrópica* em F.

O estudo da isotropia em alguns corpos é bastante simples. Por exemplo, nos corpos finitos toda forma quadrática $\rho$ tal que $\dim \rho \geq 3$ é isotrópica. Mais geralmente, conforme um resultado devido a Kneser, dado um corpo F, não formalmente real, se $|F^{\cdot}/F^2| \leq \infty$ então toda forma quadrática $\rho$ com $\dim\rho$ maior que $|\dot{F}/\dot{F}^2|$ é isotrópica.

A existência dessa cota justifica que se defina para um corpo F uma cota chamada u-*invariante*:

$$u(F) = \text{máx}\ \{\dim \rho\,;\rho \text{ é uma forma quadrática sobre } F\text{, anisotrópica em } F\}.$$

Então, para todo corpo F não formalmente real $u(F) \leq |\dot{F}/\dot{F}^2|$. É imediato, que se F é quadraticamente fechado então $u(F) = 1$ e reciprocamente.

Dois resultados importantes sobre u(F), que serão usados mais adiante nesse trabalho, e cujas demonstrações fogem do nosso objetivo, são dados em 1.22 e 1.23.

Pelo primeiro concluimos que mesmo para corpos com um número infinito de classes quadráticas é possível ter $u(F) < \infty$.

1.22 - TEOREMA (Tsen-Lang): Se $F$ é um corpo com grau de transcendência $n$ sobre um corpo algebricamente fechado então $u(F)=2^n$.

1.23 - TEOREMA (Springer): Se $K$ é uma extensão algébrica de $F$ de grau ímpar então $u(F) \leq u(K)$.

Os fatos mencionados são relativos a formas quadráticas sobre corpos não formalmente reais e referências sobre eles podem ser encontradas em [L] Capítulo VII.

Em corpos formalmente reais a situação se modifica devido a existência de ordens.

Seja $(F,P)$ um corpo ordenado e $a_1,\ldots,a_n \in P$. É fácil perceber que a forma $\rho = \langle a_1,\ldots,a_n\rangle$ é anisotrópica em F.E mais, $m\rho$ também é anisotrópica para todo $m \in \mathbb{N}$, pois, desde que $F$ é formalmente, $a_i \in P$ implica que $\sum_{i=1}^{n} a_i x_1^2 = 0$ se e somente $x_i = 0$ para todo $i = 1,\ldots,n$. Do mesmo modo $m\langle 1\rangle$ é anisotrópica, para todo $m \in \mathbb{N}$. Logo, não existe, para corpos formalmente reais, um $m \in \mathbb{N}$ tal que toda forma quadrática de dimensão maior que $m$ seja isotrópica.

Contudo, pelo Princípio de Hasse-Minkowski, num corpo de números algébricos uma forma quadrática $\rho = \langle a_1,\ldots,a_n\rangle$ com $n \geq 5$ e totalmente indefinida (isto é, tal que existam $i$ e $j$, com $1 \leq i \neq j \leq n$ para os quais $a_i a_j$ é negativo) é isotrópica.

A hipótese $\dim \rho \geq 5$ é essencial pois, a forma $\rho = \langle -3,1\rangle$, por exemplo, é totalmente indefinida (t.i.) e anisotrópica em $\mathbb{Q}$.

Essa situação, que ocorre nos corpos de números algébricos, sugere que se defina, de maneira geral, um u-invariante (também chamado, na literatura, de número de Hasse) do seguinte modo:

(1.24) $u(F) = \textit{máx}\ \{\textit{dim}\ \rho;\ \rho\ \textit{é}\ \text{t.i.}\ \textit{e anisotrópica em}\ F\}$.

Observa-se, facilmente, que para corpos não formalmente reais essa definição coincide com a anterior e que $u(F) = 4$ para todo corpo de números algébricos.

O exemplo acima mostra, também, um outro aspecto do problema de isotropia de formas quadráticas. Embora $\rho = \langle -3,1\rangle$ seja anisotrópica, $3\rho = \rho \oplus \rho \oplus \rho$ é isotrópica. Exemplos semelhantes a esse são frequentes (no conjunto dos números racionais existem muitos) e não ocorrem só em corpos de números algébricos e em corpos $F$ tais que $u(F) < \infty$.

EXEMPLO: *Seja o corpo* $\mathbb{Q}(x)$ *das funções racionais sobre* $\mathbb{Q}$ *na indeterminada* $x$. *Em* $\mathbb{Q}(x)$, *a forma* $\rho = \langle 1,x,-2x\rangle$ *é totalmente indefinida, anisotrópica e* $2\rho$ *é isotrópica.*

De fato:

i) $\rho$ é totalmente indefinida pois o produto $x(-2x)$ é negativo em todas as ordens de $\mathbb{Q}(x)$.

ii) Suponhamos que $\rho$ seja isotrópica. Então existem em $\mathbb{Q}(x)$, $\dfrac{f_1}{g_1}$, $\dfrac{f_2}{g_2}$, $\dfrac{f_3}{g_3}$, com $g_i \neq 0$ para $i = 1,2,3$ e

$f_i \neq 0$ para algum $i (1 \leq i \leq 3)$, tais que $x(\frac{f_1}{g_1})^2 + (\frac{f_2}{g_2})^2 - 2x(\frac{f_3}{g_3})^2 = \frac{1}{(g_1g_2g_3)^2}\left[x(f_1g_2g_3)^2 + (f_2g_1g_3)^2 - 2x(f_3g_1g_2)^2\right] = 0$. Mas então, $x(f_1g_2g_3)^2 + (f_2g_1g_3)^2 - 2x(f_3g_1g_2)^2 = 0$. Sejam $f_1g_2g_3 = f_1'$, $f_2g_1g_3 = f_2'$ e $f_3g_1g_2 = f_3'$. Temos: $x(f_1')^2 + (f_2')^2 - 2x(f_3')^2 = f_2'^2 + x(f_1'^2 - 2f_3'^2) = 0$. Se $\partial(f_1') \neq \partial(f_3')$ então $\partial(f_1'^2 - 2f_3'^2) = 2 \max\{\partial(f_1'), \partial(f_3')\}$. Se $\partial(f_1') = \partial(f_3') = n$, então $\partial(f_1'^2 - 2f_3'^2) = 2n$, pois, se $\partial(f_1'^2 - 2f_3'^2) < 2n$ e $f_1' = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0$ e $f_3' = b_nx^n + \ldots + b_0$ com $a_i, b_i \in Q$ então, $a_n^2 - 2b_n^2 = 0$, isto é, $(\frac{a_n}{b_n})^2 = 2$ com $a_n, b_n \in Q$, o que é uma contradição. Assim, $\partial(f_1'^2 - 2f_3'^2)$ é par e $f_1'^2 - 2f_3'^2 = 0$ implica que $f_1' = f_3' = 0$. Logo $\partial[x(f_1'^2 - 2f_3'^2)]$ é ímpar e, como $\partial(f_2'^2)$ é par, $f_2'^2 + x(f_1'^2 - 2f_3'^2) = 0$ implica que $f_2' = f_1' = f_3' = 0$. Mas então, $f_1 = f_2 = f_3 = 0$, contrariando a suposição inicial.

Portanto, $\rho$ é anisotrópica.

iii) A sextupla $(2,0,1,0,0,1)$ é solução não trivial para $2\rho = 0$. ■

No Capítulo II ficará claro que $u(Q(x)) = \infty$.

1.25 - DEFINIÇÃO: Seja $\rho$ uma forma quadrática sobre F. Se existe $m \in \mathbb{N}^*$ tal que $m\rho$ é isotrópica então dizemos que $\rho$ é fra-

*camente isotrópica*. Caso contrário, $\rho$ é chamada *fortemente anisotrópica*.

É fácil perceber que se $\rho = \langle a_1, \ldots, a_n \rangle$ então $m\rho$ ser isotrópica em $F$ significa que $\sum_{i=1}^{n} a_i \sum_{j=1}^{m} x_{ij}^2 = 0$ tem solução não trivial em $F$.

1.26 - PROPOSIÇÃO: *Sejam* $F$ *um corpo formalmente real e* $\rho = \langle a_1, \ldots, a_n \rangle$ *uma forma quadrática sobre* $F$.

$\rho$ *é fracamente isotrópica se e somente se existem* $s_1, \ldots, s_n \in \Sigma F^2$ *não todos nulos tais que* $\sum_{i=1}^{n} a_i s_i = 0$.

DEMONSTRAÇÃO: ( $\Rightarrow$ ) Se $m\rho$ é isotrópica para algum $m \geq 1$ então, existem elementos $v_{ij} \in F$, com $i = 1, \ldots, n$ e $j = 1, \ldots, m$, não todos nulos tais $\sum_{i=1}^{n} a_i \sum_{j=1}^{m} v_{ij}^2 = 0$. Tomando, para cada $i$, $s_i = \sum_{j=1}^{m} v_{ij}^2$, algum $s_i$ é diferente de zero, pois $F$ é formalmente real.

( $\Leftarrow$ ) Como $s_i \in \Sigma F^2$, $s_i = \sum_{j=1}^{m_i} v_{ij}^2$ com $v_{ij} \in F$. Seja $m = \max_{1 \leq i \leq n} \{m_i\}$ e considerando $v_{ij} = 0$ para $m \geq j > m_i$, podemos escrever $s_i = \sum_{j=1}^{m} v_{ij}^2$. Supondo que $s_i \neq 0$ para $i = i_0$, obtemos $v_{i_0 j} \neq 0$ para algum $j$. Como $\sum_{i=1}^{n} a_i \sum_{j=1}^{m} v_{ij}^2 = \sum_{i=1}^{n} a_i s_i = 0$, $\rho$ é fracamente isotrópica. ∎

Se cada $s_i$ da Proposição for não somente soma de quadrados mas um quadrado em $F$ então $\rho$ já é isotrópica. Essa situação ocorre, por exemplo, se $F$ é um corpo pitagórico ($F$ é *pitagórico* se $F^2+F^2 = F^2$). Isto é, se $F$ é pitagórico toda forma quadrática sobre $F$ que seja fracamente isotrópica é isotrópica em $F$.

A seguir, mostraremos que o estudo das formas quadráticas fracamente isotrópicas só é interessante para corpos formalmente reais.

1.27 - PROPOSIÇÃO: Seja $F$ um corpo. $F$ *não é formalmente real se e somente toda forma quadrática sobre* $F$ *é fracamente isotrópica.*

DEMONSTRAÇÃO: Seja $\rho = \langle a_1,\ldots,a_n\rangle$ uma forma quadrática sobre $F$.

Se $F$ não é formalmente real, então existe $m \in \mathbb{N} - \{0\}$ tal que $\sum_{j=1}^{m} x_j^2 = 0$ com os $x_j \in F$ e não todos nulos. Então $\rho$ é fracamente isotrópica, desde que $\sum_{i=1}^{n} a_i \sum_{j=1}^{m} x_j^2 = 0$.

Por outro lado, se $\langle 1,1\rangle$ é fracamente isotrópica então $m\langle 1,1\rangle$ é universal e $m\langle 1,1\rangle$ representa $-1$, isto é, existem $x_j \in F$ tais que $\sum_{j=1}^{m} x_j^2 = -1$. Logo, $F$ não é formalmente real. ∎

Determinar condições que assegurem a isotropia de formas quadráticas sobre um corpo é, em geral, um problema bastante difícil. Veremos que mesmo para a isotropia fraca a dificuldade ainda é grande. O próximo parágrafo estabelece condições dessa natureza.

## §4 - LEI DE SYLVESTER FRACA

Vamos definir assinatura de um corpo F com o objetivo de melhor formalizar o conceito de formas quadráticas totalmente indefinidas. No Capítulo IV essa definição também será útil.

1.28 - DEFINIÇÃO: Dado um corpo q-ordenado $(F,P)$, chama-se *assinatura de* F, relativa a q-ordem P, à função $A_P$ definida da seguinte maneira:

Para toda forma quadrática $\rho = \langle a_1,\ldots,a_n\rangle$ sobre F com $r = \#\{i;\ a_i \in P\}$ e $s = \#\{j, a_j \notin P\}$,

$$A_P(\rho) = r - s$$

Está claro, pela definição, que o valor da assinatura em $\rho$ corresponde ao número de coeficientes positivos menos o número de coeficientes negativos de $\rho$ e que $A_P(\rho) = 2r - n$.

Num estudo mais detalhado de assinaturas pode-se provar que o valor da assinatura é um invariante da classe de anisotropia da forma quadrática e que "assinatura" é um homomorfismo de anéis definido no anel de Witt do corpo.

1.29 - DEFINIÇÃO: Seja $\rho$ uma forma quadrática sobre um corpo F. Dizemos que:

a) $\rho$ é *definida* relativamente à uma q-ordem $P$ de $F$ se $|A_P(\rho)| = \dim \rho$.

b) $\rho$ é *indefinida* relativamente à uma q-ordem $P$ de $F$ se $|A_P(\rho)| < \dim \rho$.

c) $\rho$ é *totalmente indefinida* (t.i) se $|A_P(\rho)| < \dim \rho$ para toda ordem $P$ de $F$.

d) $\rho$ é *totalmente* (positivo ou negativo) *definida* se $|A_P(\rho)| = \dim \rho$ para toda ordem $P$ de $F$.

Observamos que $\rho$ é totalmente indefinida se $\rho$ é indefinida para todas as ordens e que a definição de t.i. dada aqui coincide com o conceito dado anteriormente.

Sejam os elementos $a_1,\ldots,a_n$ de um corpo $F$. Se para alguma q-ordem de $F$ todos os $a_i (1 \leq i \leq n)$ são positivos então, a equação $a_1X_1^2+\ldots+a_nX_n^2 = 0$ só admite solução trivial em $F$, visto que, se $\leq$ é uma q-ordem de $F$ então $0 < x$ implica que $0 < xy^2$, para todo $y \in \dot{F}$. Pela mesma razão, $\sum_{i=1}^{n} a_i \sum_{j=1}^{m} v_{ij}^2 = 0$ só possui solução trivial. Portanto, toda forma quadrática definida relativamente a uma q-ordem de $F$ é fortemente anisotrópica. A recíproca também vale:

1.30 - PROPOSIÇÃO: *Seja* $\rho = \langle a_1,\ldots,a_n\rangle$ *uma forma quadrática sobre* $F$. *Então,* $\rho$ *é fracamente isotrópica se e somente se* $\rho$ *é indefinida relativamente a todas as q-ordens de* $F$.

DEMONSTRAÇÃO: ( $\Rightarrow$ ) É imediata, pelos comentários anteriores à Proposição.

( $\Leftarrow$ ) Suponhamos que não existem $s_1,\dots,s_n \in \Sigma F^2$ não todos nulos tais que $\sum_{i=1}^{n} a_i s_i = 0$, isto é, que $\rho$ não é fracamente isotrópica. Seja $P_0 = \{\sum_{i=1}^{n} a_i s_i;\ s_i \in \Sigma F^2\}$. Claramente, $P_0 + P_0 \subset P_0$ e $P_0 \cdot F^2 \subset P_0$. Mas também $P_0 \cap -P_0 = \{0\}$ desde que $\sum_{i=1}^{n} a_i s_i \in P_0 \cap -P_0$ implica que $\sum_{i=1}^{n} a_i s_i = -\sum_{i=1}^{n} a_i s_i'$ para $s_i \in \Sigma F^2$. Mas então, $\sum_{i=1}^{n} a_i (s_i + s_i') = 0$ e $s_i + s_i' = 0$. Do que resulta que $s_i = s_i' = 0$. Portanto $P_0$ é um pré-q-cone de $F$ e pela Proposição 1.19, existe um q-cone $P$ de $F$ tal que $P_0 \subset P$ ou $-P_0 \subset P$. Como $a_1,\dots,a_n \in P_0$, $\rho$ é definida relativamente à $P$, o que é uma contradição. ■

Conforme já observamos, pelo Princípio Local Global de Hasse-Minkowski, num corpo $F$ de números algébricos, toda forma quadrática, totalmente indefinida, de dimensão maior ou igual a 5, é isotrópica. Assim, podemos concluir que toda forma quadrática sobre $F$, totalmente indefinida, é fracamente isotrópica.

Esse mesmo resultado pode ser obtido diretamente da Proposição 1.30.

1.31 - COROLÁRIO: *Toda forma quadrática sobre um corpo de números algébricos, totalmente indefinida é fracamente isotrópica.*

DEMONSTRAÇÃO: Basta considerar que se $F$ é um corpo de números algébricos toda q-ordem de $F$ é uma ordem e aplicar a proposição anterior. ■

O Corolário 1.31 justifica o interesse pelo seguinte princípio:

*Toda forma quadrática sobre F, totalmente indefinida, é fracamente isotrópica.*

Seja F um corpo real fechado. Como a única ordem de F é $F^2$, para uma forma quadrática $\rho$ sobre F, de dimensão n, ocorre exatamente uma das três possibilidades.

i) $\rho$ é positivo definida e nesse caso $\rho = n\langle 1\rangle$ e é anisotrópica.

ii) $\rho$ é negativo definida e nesse caso $\rho = n\langle -1\rangle$ e é anisotrópica.

iii) $\rho$ é indefinida e nesse caso $\rho = \langle 1,-1\rangle \oplus \rho'$ com $\dim\rho' = n-2$ e portanto, $\rho$ é isotrópica.

Logo, dado um corpo ordenado (F,P) uma forma quadrática sobre F é indefinida relativamente a P se e somente se ela é isotrópica no fecho real $F_P$ de F relativamente a P.

Mais ainda, uma forma quadrática $\rho$ sobre F é t.i.se e somente se ela é isotrópica em todos os fechos reais de F.

Seja $\{F_P\}$ a família dos fechos reais de F. Diremos que uma forma quadrática $\rho$ sobre F é *localmente isotrópica* se $\rho$ é isotrópica (logo, indefinida) em todos os $F_P$.

Obtemos, assim, para o princípio enunciado a seguinte formulação:

*Toda forma quadrática sobre F localmente isotrópica* *é fracamente isotrópica em* F.

E o chamaremos de *Lei de Sylvester Fraca* (L.S.F.).

Pelo Corolário 1.31 um exemplo de corpos nos quais vale a L.S.F. são os corpos de números algébricos. No Capítulo II apresentaremos mais exemplos.

A L.S.F. é um princípio análogo ao Princípio Local Global de Pfister que caracteriza os elementos de torção do anel de Witt de F. Mas, enquanto, o Princípio de Pfister vale para todos os corpos formalmente reais, a L.S.F. é válida, conforme mostraremos no Teorema 1.32, numa classe restrita de corpos.

Para facilitar o nosso trabalho daqui em diante, denotaremos por:

$Y_F$ o conjunto das q-ordens de F.

$X_F$ o conjunto das ordens de F.

Convém notar que $X_F \subset Y_F$, qualquer que seja F.

1.32 - TEOREMA: *Seja* F *um corpo formalmente real. São equivalentes:*

1) *Toda* q-*ordem de* F *é uma ordem, isto é,* $X_F = Y_F$.

2) *A* L.S.F. *vale em* F, *isto é, toda forma quadrática sobre* F *localmente isotrópica é fracamente isotrópica em* F.

3) *Toda forma quadrática* $\rho$ *sobre* F *tal que* $\rho^s$ *é fracamente isotrópica para algum* $s \geq 1$ *é fracamente isotrópica em* F.

4) *Toda forma quadrática do tipo* $<1,a,b,-ab>$ *é fracamente isotrópica em* F.

OBSERVAÇÃO: $\rho^s$ denota a forma $\rho \otimes \rho \otimes \ldots \otimes \rho$ (s vezes).

DEMONSTRAÇÃO:

1) $\Rightarrow$ 2) Seja $\rho$ uma forma quadrática sobre F localmente isotrópica. Por 1) $\rho$ é indefinida em relação a todas as q-ordens de F, e então, pela Proposição 1.30, $\rho$ é fracamente isotrópica.

2) $\Rightarrow$ 3) Se $m\,\rho^s$ é isotrópica para algum $m \geq 1$ então $\rho$ é totalmente indefinida e, por 2), $\rho$ é fracamente isotrópica.

3) $\Rightarrow$ 4), Seja $\rho = <1,a,b,-ab>$. A forma $\rho^2 = <1,a,b,-ab, a,a^2,ab,-ab^2,\ldots,a^2b^2>$ é isotrópica. Então, por 3), $\rho$ é fracamente isotrópica.

4) $\Rightarrow$ 1) Suponhamos que P é uma q-ordem própria de F. Então, existem $x,y \in P$ tais que $xy \in -P$, isto é, $<1,x,y,-xy>$ é definida relativamente a P e é portanto, por 1.30, fortemente anisotrópica, contrariando 4). ■

O Teorema 1.32 nos permite concluir que para o u-invariante (conforme definido em 1.24) de $Q(x)$ vale $u(Q(x)) = \infty$, pois, como $Q(x)$ possui q-ordem própria (isso ficará claro no Capítulo II) existem formas quadráticas sobre $Q(x)$, totalmente indefinidas, que não são fracamente isotrópicas. Portanto, não existe $m \in \mathbb{N}$ tal que toda forma quadrática sobre $Q(x)$, de dimensão maior que m e t.i., seja isotrópica.

De modo semelhante podemos concluir que $u(\mathbb{R}(x,y)) = \infty$ (no Capítulo II daremos um exemplo de q-ordem própria de $\mathbb{R}(x,y)$).

O Corolário 1.33, a seguir, é a versão do Teorema 1.32 para corpos pitagóricos. Usando o teorema mostraremos que podemos assegurar a isotropia em F, de uma forma quadrática sobre F sabendo que ela é localmente isotrópica somente quando F é pitagórico e não possui q-ordens próprias.

1.33 - COROLÁRIO: *Seja* F *um corpo formalmente real. São equivalentes:*

1') F *é pitagórico e* $X_F = Y_F$

2') *Toda forma quadrática sobre* F *localmente isotrópica é isotrópica em* F.

3') *Toda forma quadrática* $\rho$ *sobre* F *tal que* $\rho^s$ *é isotrópica para algum* $s \in \mathbb{N}^{\bullet}$, *é isotrópica em* F.

DEMONSTRAÇÃO:

1') $\Rightarrow$ 2') Decorre do Teorema 1.32, desde que num corpo pitagórico os conceitos de forma quadrática isotrópica e fracamente isotrópica coincidem.

2') $\Rightarrow$ 3') Se $\rho^s$ é isotrópica então $\rho$ é t.i. e, portanto, por 2'), $\rho$ é isotrópica.

3') $\Rightarrow$ 1') Basta provar que F é pitagórico pois $X_F = Y_F$ decorre da Proposição. Sejam $a,b,c \in F^{\cdot}$ tais que $a^2 + b^2 = c$ e a forma quadrática $\rho = \langle 1,-c \rangle$. Em F, $(0,\frac{a}{c},\frac{b}{c},\frac{1}{c})$ é solução não trivial para $\rho^2 = \langle 1,-c,-c,c^2 \rangle$. Então, por 3), $\rho$ é isotrópica e portanto $c \in \dot{F}^2$. ■

No Corolário 1.33 não pode ser incluido 4': Toda forma quadrática do tipo $\langle 1,a,b,-ab \rangle$ sobre $F$ é isotrópica. Em $\mathbb{R}(x)$ toda forma quadrática desse tipo é isotrópica (ver capítulo IV) e $\mathbb{R}(x)$ não é pitagórico, pois $1 + x^2$ não é quadrado em $\mathbb{R}(x)$. Por outro lado, a hipótese de $F$ ser pitagórico é essencial, pois para $F = Q$, $X_F = Y_F$ e não vale 1.33 (2').

O Teorema 1.32 e o Corolário 1.33 mostram que se $\rho$ é localmente isotrópica podemos garantir que $m\rho$ seja isotrópica somente se impusermos a condição $X_F = Y_F$ sobre o corpo e, para garantir a isotropia de $\rho$ precisamos restringir mais ainda os corpos.

No entanto, veremos agora, que, se $\rho$ é localmente isotrópica então $\rho^n = \rho \otimes \rho \otimes \ldots \otimes \rho$ (n vezes) sempre é fracamente isotrópica. Esse resultado é obtido como Corolário da seguinte proposição:

1.34 - PROPOSIÇÃO: *Seja $F$ um corpo formalmente real $\rho = \langle a_1,\ldots,a_n \rangle$ uma forma quadrática sobre $F$. Se $\rho^n$ é localmente isotrópica então $\rho^n$ é fracamente isotrópica em $F$.*

DEMONSTRAÇÃO: Suponhamos que $\rho^n$ seja fortemente anisotrópica e seja $P_0 = \{ \sum_{i=1}^{t} \prod_{j=1}^{n} (b_{ij}) x_i^2 ;\ t \in \mathbb{N},\ x_i \in F \text{ e } b_{ij} \in \{a_1,\ldots,a_n\} \}$.

Como para todo $m \in \mathbb{N}$, $m\rho^n$ é anisotrópica, $P_0 \cap -P_0 = \{0\}$. Além disso $P_0$ possui as propriedades: $P_0 + P_0 \subset P_0, P_0 . P_0 \subset P_0$ e $F^2 \subset P_0$ (basta supor, sem perda de generalidade $a_1=1$, escolher $t = 1$ e tomar $b_{ij} = a_1$ para todo $j = 1,\dots,n$). Logo $-1 \notin P_0$ e $P_0$ é um pré-cone de F. Como, $P_0$ se estende a uma cone P de F temos em F uma ordem relativa a qual $\rho^n$ é definida. Mas então, $\rho^n$ não é isotrópica no fecho real $F_P$ de $(F,P)$, contrariando a hipótese. Logo $\rho^n$ é fracamente isotrópica. ■

1.35 - COROLÁRIO: *Seja F um corpo formalmente real. Se a forma quadrática $\rho = \langle a_1,\dots,a_n \rangle$ sobre F é localmente isotrópica então $\rho^n$ é fracamente isotrópica em F.*

DEMONSTRAÇÃO: Como $\rho$ é t.i., $\rho^n$ também é t.i. e, por 1.34, $\rho^n$ é fracamente isotrópica. ■

O Teorema 1.32 justifica o estudo das q-ordens de um corpo, mas não dá um critério prático para determinar corpos que satisfazem a L.S.F., porque, em geral, não são conhecidas explicitamente todas as q-ordens de um corpo. No Capítulo II daremos um critério, para determinar os corpos que não possuem q-ordens próprias, usando valorizações reais.

# CAPÍTULO II

## CARACTERIZAÇÃO DE CORPOS QUE SATISFAZEM A LEI DE SYLVESTER FRACA

No primeiro parágrafo desse Capítulo são caracterizados, através de valorizações reais, os corpos que não possuem q-ordem própria (Teorema 2.25); no segundo parágrafo, é dada uma caracterização de corpos henselianos que não possuem q-ordem própria (Teorema 2.45); e no §3 são analisados exemplos.

### §1 - VALORIZAÇÕES E q-ORDENS

Na definição de valorização é usado o conceito de grupo ordenado.

Seja $G$ um grupo aditivo. Dizemos que $G$ é um *grupo ordenado* se existe $S \subset G$ tal que $S + S \subset G$, $S \cup (-S) = G$ e $S \cap -S = \{0\}$.

O conjunto $S$ define em $G$ uma relação binária $\leq$ dada por:

$$g_1 \leq g_2 \leftrightarrow g_1 - g_2 \in S$$

e que satisfaz:

(i) $\leq$ é uma relação de ordem total, isto é:

a) $g \leq g$ para todo $g \in G$

b) $g_1 \leq g_2$ e $g_2 \leq g_1 \Rightarrow g_1 = g_2$, para $g_1, g_2 \in G$

c) $g_1 \leq g_2$ e $g_2 \leq g_3 \Rightarrow g_1 \leq g_3$, para $g_1, g_2, g_3 \in G$.

d) $g_1 \nleq g_2 \Rightarrow g_2 < g_1$, para $g_1, g_2 \in G$.

(ii) $\leq$ é compatível com a operação de $G$, isto é, se $g_1, g_2 \in G$ e $g_1 < g_2$ então, $g_1 + g < g_2 + g$, para todo $g \in G$.

Reciprocamente, toda relação binária que satisfaz (i) e (ii) determina em $G$ o conjunto $S = \{g \in G; g \geq 0\}$ com as propriedades $S + S \subset S$, $S \cup (-S) = G$ e $S \cap -S = \{0\}$.

Como a correspondência acima é biunívoca chamaremos indistintamente $\leq$ e $S$ de *ordem* de $G$, e denotaremos o grupo ordenado por $(G,S)$ ou $(G,\leq)$ quando quisermos por em evidência a ordem que está sendo considerada.

Exemplos de grupos ordenados são o grupo aditivo e o grupo multiplicativo de um corpo ordenado. Outro exemplo é $(\mathbb{Z},+)$. Um grupo $(G,\cdot)$ é arquimediano se dados $g \in G$ e $0 < h \in G$, existe $n \in \mathbb{N}$ tal que $nh > g$.

Os grupos $(\mathbb{Z},+)$, $(\mathbb{Q},+)$ e $(\mathbb{Q}^{\cdot},.)$ são arquimedianos. O grupo $(\mathbb{Z} \times \mathbb{Z},+)$, com a ordem lexicográfica: $(a,b) \leq (c,d) \leftrightarrow a < c$ ou $a = c$ e $b \leq d$, é não arquimediano.

2.1 - DEFINIÇÃO: *Seja* $F$ *um corpo. Uma aplicação sobrejetora* $v : \dot{F} \to G$ *definida no conjunto dos elementos não nulos de* $F$ *e assumindo valores num grupo aditivo abeliano ordenado* $G$, *se diz uma valorização de* $F$ *se:*

(i) $v$ *é um homomorfismo do grupo multiplicativo* $\dot{F}$ *no grupo* *aditivo* $G$, *isto é*, $v(ab) = v(a) + v(b)$ *para todos* $a,b \in \dot{F}$.

(ii) $v(a + b) \geq min\{v(a), v(b)\}$ *para* $a,b \in \dot{F}$ *tais que* $a + b \in \dot{F}$.

O grupo $G$ é chamado *grupo de valores de* $v$. O par $(F,v)$- ou a tripla $(F,v,G)$ conforme queiramos ou não realçar o grupo de valores - se diz um *corpo valorizado*.

Convencionando $v(0) = \infty$ e definindo em $G \cup \{\infty\}$ as regras usuais para o símbolo $\infty$, ou seja $g < \infty$ e $g + \infty = \infty + g = \infty + + \infty = \infty$ para todo $g \in G$, podemos estender a aplicação $v$ a todo $F$.

Algumas consequências imediatas da definição, frequentemente usadas ao se tratar com valorizações, são:

$v(1) = 0$, $v(-x) = v(x)$, $v(x^{-1}) = -v(x)$ e

$v(x) < v(y) \Rightarrow v(x + y) = v(x)$ para $x,y \in F$.

Para toda valorização $v : \dot{F} \to G$ existe um anel local a ela associado. É o anel

$A_v = \{x \in F,\ v(x) \geq 0\} \cup \{0\}$ : = anel *da* valorização $v$, cujo ideal maximal é

$M_v = \{x \in F;\ v(x) > 0\} \cup \{0\}$: = ideal maximal *da* valorização $v$.

O anel quociente $A_v/M_v$ é um corpo (pois $M_v$ é um ideal maximal de $A_v$) chamado *corpo de restos* ou *corpo das classes residuais* de $v$ e será denotado por $F_v$. Se $a \in A_v$, denotamos por $\bar{a}$ o elemento $a + M_v \in F_v$.

Notemos que $A_v$ é um subanel unitário de $F$ cujo corpo de frações é $F$ e que $A_v$ é um *anel de valorização de* $F$, isto é, $A_v$ é um subanel de $F$ que contém o "1" e satisfaz: $a \notin A_v \Rightarrow$ $\Rightarrow a^{-1} \in A_v$, para todo $a \in \dot{F}$.

O inverso também é verdadeiro, isto é, dado um anel de valorização $A$ de $F$ podemos definir em $F$ uma valorização $v$ tal que $A$ seja o anel a ela associado. De fato:

Seja $A$ um anel de valorização de $F$ e $U = \{x \in A;$ $x^{-1} \in A\}$ o grupo das unidades de $A$. O grupo $G = \dot{F}/U$ é um grupo totalmente ordenado, pela relação $xU < yU \leftrightarrow x^{-1}y \in M$ onde $M = \{x \in A;\ x^{-1} \notin A\}$ é o conjunto das não unidades de $A$. Escrevendo $G$ aditivamente o homomorfismo canônico $v : \dot{F} \to \dot{F}/U$ é uma valorização de $F$ cujo anel é $A$.

A valorização associada a $A$ é única, a menos de equivalência, pois, se $A$ é um anel de valorização de $F$, $A$ é um anel local cujo único ideal maximal é $M = \{x \in A;\ x^{-1} \notin A\}$. Para verificar isso basta lembrar a definição de valorizações equivalentes.

Dizemos que duas *valorizações* $v : \dot{F} \to G$ e $v' : \dot{F} \to G'$ são *equivalentes* se existe um isomorfismo $\varphi$ de grupos ordenados entre $G$ e $G'$ tal que $v' = \varphi \circ v$, isto é, tal que o seguinte diagrama é comutativo.

$$\begin{tikzcd} & \dot{F} \arrow[dl, "v"'] \arrow[dr, "v"] & \\ G \arrow[rr, "\varphi"] & & G' \end{tikzcd}$$

Seja, agora, $w : \dot{F} \to G$ uma valorização de $F$ tal que $A_w = A$. O núcleo do homomorfismo sobrejetor $w$ é o conjunto

$U_w = \{x \in A;\ x^{-1} \in A\}$ das unidades de $A_w = A$. Logo $G \simeq \dot{F}/U_w = \dot{F}/U$ e, portanto, $w$ é equivalente a $v$.

Com isso concluímos que duas valorizações que correspondem ao mesmo anel de valorização são equivalentes e que existe uma correspondência um a um entre as valorizações, a menos de equivalência, e os anéis de valorização de um corpo. Assim, salvo menção em contrário, trabalharemos sempre com classes de equivalência de valorizações.

Algumas informações sobre valorizações podem ser obtidas estudando seu grupo de valores. Com esse objetivo damos a definição 2.2 e os resultados 2.3 e 2.4.

2.2 - DEFINIÇÃO: *Seja* $G$ *um grupo abeliano ordenado. Um subgrupo* $H$ *de* $G$ *é um subgrupo convexo (ou isolado) de* $G$ *se* $g \in G, h \in H$ *com* $0 < g \leq h$ *implica que* $g \in H$, *ou seja,* $\{g \in G;\ 0 \leq g \leq h\} \subset H$ *para todo* $h \in H$.

Em particular $\{0\}$ e $G$ são subgrupos convexos de $G$.

2.3 - PROPOSIÇÃO: *Seja* $G$ *um grupo abeliano ordenado. A família dos subgrupos convexos de* $G$ *é totalmente ordenada em relação à inclusão.*

DEMONSTRAÇÃO: Sejam $G_1$ e $G_2$ dois subgrupos convexos de $G$ com $G_1 \not\subset G_2$. Então, existe $g_1 \in G_1$ tal que $g_1 \notin G_2$. Para todo $g_2 \in G_1$ temos que $g_2 < g_1$ e, portanto, $g_2 \in G_1$. Assim, $G_2 \subset G_1$ ■

Na teoria dos grupos abelianos ordenados os subgrupos convexos tem um papel semelhante ao dos subgrupos normais na teoria de grupos arbitrários.

2.4 - PROPOSIÇÃO: *Seja* $(G,P)$ *um grupo abeliano ordenado e* $H$ *um subgrupo convexo de* $G$. *O grupo quociente* $G/H$ *pode ser munido de uma estrutura de grupo ordenado de modo que a projeção canônica* $\pi : G \to G/H$ *seja um epimorfismo de grupos ordenados.*

DEMONSTRAÇÃO: Basta verificar que o conjunto $\bar{P} = \{\pi(p);\ p \in P\} = \{p + H;\ p \in P\}$ define em $G/H$ uma estrutura de grupo ordenado preenchendo as condições do teorema.■

Observemos que $\bar{P}$ define em $G/H$ a relação binária dada por $\bar{g}_1 < \bar{g}_2 \leftrightarrow \bar{g}_1 \neq \bar{g}_2$ e $g_1 < g_2$.

Observemos, também, que pela definição de $\bar{P}$ temos que $P^{\cdot} \subset \{p \in G;\ \bar{p} \in \bar{P}^{\cdot}\}$. Mas, desde que $\bar{P}$ é uma ordem, vale a igualdade $P^{\cdot} = \{p \in G;\ \bar{p} \in \bar{P}\}$. De fato: Assumamos que $\bar{p} \in \bar{P}$. Se $p \notin P$ então $-p \in P$ e $-\bar{p} \in \bar{P}$, o que contradiz $\bar{P}$ ser uma ordem. Logo, se $\bar{p} \in \bar{P}$ então $p \in H$ ou $p \in P$.

Nosso objetivo (que será alcançado em 2.27) é estabelecer uma relação entre q-ordens próprias e ordens através de valorizações.

2.5 - DEFINIÇÃO: *Sejam* $v : \dot{F} \to G$ *uma valorização e* $P$ *uma q-ordem de* $F$. *Dizemos que* $P$ *é compatível com* $v$ *(ou* $v$ *é compatível com* $P$*) se* $b-a \in P^{\cdot}$ *implica em* $v(a) \geq v(b)$. *Ou,* (conforme usaremos nuitas vezes), *se* $a \in P^{\cdot}$ e $v(a) < v(b)$ *implicar que*

$a - b \in P$.

Na proposição abaixo estaremos usando o fato de que o corpo q-ordenado (F,P) em relação à sua estrutura aditiva é um grupo ordenado.

2.6 - PROPOSIÇÃO: *Sejam* (F,v,P) *um corpo valorizado* q-*ordenado e as afirmações abaixo:*

(i) *A* q-*ordem* P *é compatível com* v.

(ii) *O subgrupo* $(A_V,+)$ *é um subgrupo convexo de* $(F, +)$.

(iii) *O subgrupo* $(M_V, +)$ *é um subgrupo convexo de* $(A_V, +)$.

Então:

a) *Se* P *for uma* q-*ordem própria de* F *então* (i) $\Rightarrow$ (ii) $\Longleftrightarrow$ $\Longleftrightarrow$(iii).

b) *Se* P *for uma ordem de* F *então* (i),(ii) e (iii) *são equivalentes*.

A demonstração é imediata e pode ser encontrada em [P ] (1975) Teorema 7.2 .

Convém notar que se P é uma q-ordem própria de F, a implicação (ii) $\Rightarrow$ (i) pode não ocorrer (ver exemplo 2.48).

Em 2.8, vamos mostrar que sob *certas restrições* sobre o grupo de valores G de v as afirmações (i),(ii) e (iii) também são equivalentes se P for uma q-ordem própria. Para isso, demonstraremos a Proposição 2.7.

OBSERVAÇÃO: Passaremos a usar a expressão "A é convexo em relação a q-ordem P de F" para significar que o subgrupo $(A,+)$ é um subgrupo convexo do grupo aditivo $(F,+)$.

2.7 - PROPOSIÇÃO: *Seja* $(F,v,G,P)$ *um corpo valorizado* q-*ordenado tal que* $A_v$ *é convexo em relação a* P. *Dados* $a,b \in F$ *com* $a \in P$ *e* $v(a) \neq v(b)$, *se existe* $g \in G$ *tal que* $v(a) \leq 2g \leq v(b)$ *então* $a - b \in P$.

DEMONSTRAÇÃO: Sejam $b \in P$ e $c \in F$ tal que $v(c) = g$. Logo, $2g = v(c^2)$ e por hipótese $v(a) \leq v(c^2) \leq v(b)$. Temos, então, $v(ac^{-2}) \leq 0 \leq v(bc^{-2})$. Como $v(a) \neq v(b)$ a igualdade não vale simultaneamente nos dois lados:

1º CASO: $v(ac^{-2}) < 0 \leq v(bc^{-2})$

Temos $bc^{-2} \in A_v$ e $ac^{-2} \notin A_v$. De $a \in P^{\bullet}$ e da convexidade de $A_v$ obtemos $ac^{-2} - bc^{-2} \in P$ e, portanto, $a - b \in P$.

2º CASO: $v(ac^{-2}) \leq 0 < v(bc^{-2})$.

Temos $bc^{-2} \in M_v$, mas $ac^{-2} \notin M_v$. Desde que a convexidade de $A_v$ relativamente a P implica na convexidade de $M_v$ relativamente a P temos que $ac^{-2} - bc^{-2} \in P$ e, portanto, $a - b \in P$. ∎

2.8 - COROLÁRIO: *Seja* $(F,v,G,P)$ *um corpo valorizado* q-*ordenado tal que* $A_v$ *é convexo em relação a* P. *Se para todos* $g_1, g_2 \in G$ *tais que* $g_1 < g_2$ *existe* $g \in G$ *com* $g_1 \leq 2g \leq g_2$, *então* P *é compatível com* v.

DEMONSTRAÇÃO: Decorre imediatamente da proposição 2.7.

Particularmente, esse resultado mostra que se $o(G/2G)=1$, isto é, se $G$ é 2-divisível então, a valorização $v$ é compatível com a q-ordem $P$. O mesmo ocorre se $G \cong \mathbb{Z}$.

2.9 - DEFINIÇÃO: *Seja* $v : \dot{F} \to G$ *uma valorização não trivial de* $F$. *Dizemos que* $v$ *é uma valorização real se o corpo residual* $F_v$ *é formalmente real.*

Mostraremos agora que, independente de $P$ ser q-ordem própria ou ordem, se for válida qualquer uma das três condições da Proposição 2.6, então o corpo de resíduos de $v$ é formalmente real.

2.10 - PROPOSIÇÃO: *Seja* $(F,v,P)$ *um corpo valorizado q-ordenado tal que* $A_v$ *é convexo relativamente a* $P$. *O corpo residual* $F_v$ *é formalmente real.*

DEMONSTRAÇÃO: Desde que o grupo aditivo $(A_v,+)$ é totalmente ordenado com a ordem $A_v \cap P$ induzida pela q-ordem de $F$ e como por 2.6, $(M_v,+)$ é um subgrupo convexo de $A$ temos, por 2.4, que $F_v = A_v/M_v$ é ordenado, como grupo aditivo, por $\bar{P}=A_v \cap P/M_v$. Resta então provar que $\bar{F}_v^2\,\bar{P} \subset \bar{P}$. Observemos primeiro que $P \cap A_v^{\bullet} = \{p \in A_v;\ \bar{p} \in \bar{P}^{\bullet}\}$, isto é, se $\bar{a} \in \bar{P}$ então $a \in M_v$ ou $a \in P$. Sejam $\bar{a} = a + M_v \in F_v$ e $\bar{b} = b + M_v \in \bar{P}$. Se $\bar{b} = M_v$ é imediato que $\bar{a}^2 \,.\, \bar{b} \in \bar{P}$. Se $\bar{b} \neq M_v$ então $b \in P \cap A_v^{\bullet}$ e como $a \in A_v$ temos $a^2b \in P \cap A_v$. Assim $\overline{a^2b} = \bar{a}^2 .\, \bar{b} \in \bar{P}$ e $\bar{P}$ é uma q-ordem de $F_v$. Logo, pelo Corolário 1.21, $F_v$ é formalmente real.∎

Por outro lado, só corpos formalmente reais possuem valorizações reais.

2.11 - PROPOSIÇÃO: *Seja* F *um corpo. Se existe uma valorização real* v *de* F *então* F *é formalmente real.*

DEMONSTRAÇÃO: Seja A o anel da valorização v e M o ideal maximal de A. Suponhamos que F não é f.r.. Então existe uma relação da forma $\sum_{i=1}^{n} a_i^2 = 0$ com $a_i \in \dot{F}$. Seja $a_t$ tal que $v(a_t) \leq v(a_i)$ para qualquer i. Temos $a_t \neq 0$ e dividindo $\sum_{i=1}^{n} a_i^2 = 0$ por $a_t^2$ obtemos $-1 = \sum_{i \neq t} b_i^2$ onde $b_i = \frac{a_i}{a_t}$. Assim, $v(b_i) = v(a_i) - v(a_t) \geq 0$ e $b_i \in A$ para todo $i \neq t$. Logo, $b_i^2 \in A$ e $-\bar{1} = \sum \bar{b}_i^2$, contradizendo $F_v$ ser formalmente real. ∎

2.12 - PROPOSIÇÃO: *Seja* (F,P) *um corpo q-ordenado. Se* P *é compatível com alguma valorização real* v *de* F *então* P *é não arquimediana.*

DEMONSTRAÇÃO: Suponhamos que P é compatível com a valorização $v : \dot{F} \to G$. Sejam $g \in G$ tal que $g < 0$ e $a \in P^{\cdot}$ tal que $v(a) = g$. Como, para qualquer que seja $n \geq 1$, vale $v(n) \geq 0$, temos que $v(a) < v(n)$ e, portanto, pela compatibilidade de v em relação a P, $n \leq a$ para todo $n \in \mathbb{N}$. ∎

Vamos mostrar agora que, dada uma q-ordem não arquimediana P de F, sempre é possível associar a P uma valorização real $v : \dot{F} \to G$ de F. O que vamos fazer, na verdade, é estabelecer um processo de construção de anéis de valorização real. Mais adiante veremos que todos os anéis de valorização real podem ser obtidos dessa maneira.

Lembramos que o valor absoluto relativo a uma q-ordem P é definido como usualmente: $|a| = a$ se $a \in P$ e $|a| = -a$ se $a \notin P$, ou seja, $|a| = \text{máx.}\{a,-a\}$ .

2.13 - PROPOSIÇÃO: *Sejam* $(F,\leq)$ *um corpo q-ordenado e* k *um subcorpo de* F. *O conjunto* $A(\leq,k) = \{x \in F; |x| \leq a$ *para algum* $a \in k\}$ *é um anel de valorização de* F, *convexo em relação a* $\leq$.

DEMONSTRAÇÃO: Sejam $x,y \in A(\leq,k)$. Temos: $|x| \leq a$ para algum $a \in k$ e $|y| \leq b$ para algum $b \in k$. Então, $|x + y| \leq |x| + |y| \leq$ $\leq a + b \in k$, isto é, $x + y \in A(\leq,k)$. Além disso, $|x.y| = |(\frac{x+y}{2})^2 -$ $- (\frac{x-y}{2})^2| \leq (\frac{x+y}{2})^2 + (\frac{x-y}{2})^2 \in A(\leq,k)$ pois, se $\alpha \in A(\leq,k)$ então $\alpha^2 \in A(\leq,k)$. De fato: Se $\alpha \in A(\leq,k)$, existe $b \in k$ (podemos supor $b > 1$) tal que $|\alpha| \leq b$. Por 1.14(vii), $|\alpha| < b^2$ e, portanto, por 1.14(v), $|\alpha^2| = |\alpha|^2 < b^4 \in k$, isto é, $\alpha^2 \in A(\leq,k)$.

Se $x \in \dot{F}$ e $x \notin A(\leq,k)$ então, $a < |x|$, para todo $a \in k$. Donde, por 1.14(iii), $|x^{-1}| < |a|$, para todo $a \in \dot{k}$, e portanto, $x^{-1} \in A(P,k)$.

Se $0 < a \leq b \in A(\leq,k)$ então existe $\alpha \in k$ tal que $|b| \leq \alpha$. Consequentemente $|a| \leq \alpha$ com $\alpha \in k$ e, portanto, $a \in A(\leq,k)$.

Logo, $A(\leq,k)$ é um anel de valorização de F, convexo em relação a $\leq$. ∎

Claramente, o ideal maximal de $\dot{A}(\leq,k)$ é o conjunto $M(\leq,k) = \{x \in F;\ |x| < |a| \text{ para todo } a \in \dot{k}\}$, pois $x \in \dot{A}(\leq,k)$ e $x^{-1} \notin \dot{A}(\leq,k)$ implica que $|x^{-1}| > |a|$ para todo $a \in \dot{k}$ e, portanto, $|x| < |a|$, para todo $a \in \dot{k}$.

Na literatura ([La]), se $\leq$ for uma ordem, os elementos de $M(\leq,k)$ são chamados *infinitamente pequenos* sobre k (notação: $x << k$) e os elementos de $A(\leq,k)$ são os elementos de F que não são *infinitamente grandes* sobre k (notação: $x \not>> k$). Os elementos do grupo das unidades de $A(\leq,k)$, isto é, de $U(\leq,k) = A(\leq,k)\setminus M(\leq,k)$ são os elementos x de F para os quais existem $a,b \in k$ tais que $0 < |a| \leq x \leq |b|$. $U(\leq,k)$ é, portanto, o conjunto dos elementos de F que não são infinitamente grandes e nem infinitamente pequenos sobre k.

Observemos que, desde que F é formalmente real, $Q \subseteq k \subseteq F$ e, portanto, $Q \subseteq A(P,k)$.

Se P for uma q-ordem arquimediana (portanto, uma ordem) então $A(P,k) = F$, e a valorização $v: \dot{F} \to G$ associada a $A(P,k)$ é dada por $v(x) = 0$ para todo $x \in \dot{F}$. Quando isso ocorre dizemos que k é *cofinal* em F em relação a P (ou F é arquimediano sobre k, [La]). Isto é, *um corpo* k *é cofinal em* F *relativamente a uma q-ordem* P *se para todo* $x \in F$, *existe* $a \in k$ *tal que* $|x| \leq a$.

Se P for uma q-ordem não arquimediana então $A(P,k) \subsetneq F$ e, pela Proposição 2.10, a valorização associada é uma valorização real.

Desde que $A(P,k)$ é convexo em relação a P, pela Proposição 2.10, podemos concluir que dada uma ordem P não arquimediana de F sempre é possível obter uma valorização real de F que, pela Proposição 2.6, é compatível com P. De modo que, pela Proposição 2.12, vale para ordens o seguinte teorema.

2.14 - TEOREMA: *Seja* (F,P) *um corpo ordenado*. P *é uma ordem não arquimediana se e somente se existe uma valorização real de* F *compatível com* P.

Se P for uma q-ordem própria não arquimediana então a valorização associada ao anel A(P,k) nem sempre é compatível com P (Exemplo 2.48). Porém, conforme constatamos em 2.8, colocando hipóteses sobre o grupo de valores é possível obter também, para q-ordens a compatibilidade mencionada. Na Proposição 2.15 mostraremos que, se o grupo de valores da valorização associada ao anel A(P,Q) é tal que o $(G/2G) \leq 2$, então é possível obter uma valorização real de F compatível com P.

2.15 - PROPOSIÇÃO: *Sejam* P *uma* q-*ordem não arquimediana de* F *e* $v : \dot{F} \to G$ *a valorização real associada ao anel de valorização* A(P,Q). *Se* $o(G/2G) \leq 2$ *então existe uma valorização real* $w : \dot{F} \to G_1$ *tal que* P *é compatível com* w *e* $o(G_1/2G_1) = o(G/2G)$.

DEMONSTRAÇÃO: Seja $o(G/2G) = 1$. Como A(P,Q) é convexo em relação a P e para todo $g \in G$ existe $g_0 \in G$ tal que $g = 2g_0$, pelo Corolário 2.8, P é compatível com v.

Seja $o(G/2G)=2$ e $g_0 \in G/2G$ com $g_0 > 0$. Definimos $G' = \{g \in G$ para os quais não existe $g_1 \in G$ tal que $0 \leq g_0 +$

$+ 2g_1 < 2|g|$.

(i) $G'$ é um subgrupo de $G$.

Sejam $g', g'' \in G'$ com $|g'| \leq |g''|$. Suponhamos que $g' - g'' \notin G'$. Então existe $g_1 \in G$ tal que $0 \leq g_0 + 2g_1 < 2|g-g''|$. Como $g'' \in G'$ temos $g_0 + 2g_1 \geq 2|g''|$ e, portanto, $0 \leq g_0 + 2(g_1 - |g''|)$. Por outro lado, $g_0 + 2g_1 < 2|g' - g''|$ implica em $g_0 + 2g_1 < 2|g'| + 2|g''|$ e então $g_0 + 2g_1 < 2|g''| + 2|g''|$, isto é, $g_0 + 2(g_1 - |g''|) < 2|g''|$. Mas $0 \leq g_0 + 2(g_1 - |g''|) < 2|g''|$ contradiz $g'' \in G$. Logo $g' - g'' \in G'$.

(ii) $G'$ é convexo em $G$ relativamente a ordem $\leq$ de $G$.

Sejam $g' \in G$ e $g \in G'$ com $0 < g' \leq g$. Então, para qualquer $g_1 \in G$ tal que $0 \leq g_0 + 2g_1$ vale $g_0 + 2g_1 \geq 2|g| = 2g$ e, portanto, para qualquer $g_1 \in G$ tal que $0 \leq g_0 + 2g_1$ vale $g_0 + 2g_1 \geq 2g' = 2|g'|$. Logo $g' \in G'$.

Assim, por 2.4, o grupo quociente $G_1 = G/G'$ pode ser munido de uma estrutura de grupo ordenado, pela relação $g_1 + G' < g_2 + G' \leftrightarrow g_1 - g_2 \notin G'$ e $g_1 < g_2$, de modo a tornar a projeção canônica $G \to G_1$, $g \to \bar{g} = g + G'$, um epimorfismo de grupos ordenados. A aplicação $w : \dot{F} \to G_1 = G/G'$, $x \to v(x) + G'$, é uma valorização de $F$.

Mostremos, agora, que $w$ é compatível com $P$.

Sejam $x \in F$, $y \in F$ com $x > 0$ e $w(x) < w(y)$. Então, $v(x) < v(y)$ e $v(x) - v(y) \notin G'$. Se $v(x) \in 2G$ ou $v(y) \in 2G$ temos $v(x) \leq 2g \leq 2(y)$ para algum $g \in G$ e, então, como $A(P,Q)$ é convexo, pela Proposição 2.7, $y < x$. Suponhamos que $v(x) \notin 2G$ e

$v(y) \notin 2G$. Como $o(G/2G) = 2$ e $g_0 \notin 2G$ temos $v(x) = g_0 + 2g_1$ e $v(y) = g_0 + 2g_2$ com $2g_1 < 2g_2$. Mas, $2g_1 - 2g_2 = v(x) - v(y) \notin G'$ e, portanto, $g_1 - g_2 \notin G'$. Logo, existe $g_3 \in G$ tal que $0 < g_0 + 2g_3 < 2(g_2 - g_1)$. Assim, $v(x) = g_0 + 2g_1 \leq 2(g_0 + g_1 + g_3) < g_0 + 2g_2 = v(y)$ e, pela Proposição 2.7, $y < x$. Logo, $w$ é compatível com $P$ e, portanto, pela Proposição 2.6 e Proposição 2.10, o corpo de resíduos $F_w = A_w/M_w$ é formalmente real, isto é, $w$ é uma valorização real.

De $o(G/2G) = 2$ temos $G' \subset 2G$ pois para todo $g \in G \setminus 2G$ e $g > 0$, existe $h \in G$ tal que $g = g_0 + 2h$ e, portanto, $0 < g_0 + 2h < 2|g|$, isto é, $g \notin G'$. (O grupo $G'$ é, na verdade, o subgrupo de $G$ convexo maximal contido em $2G$.) E, de $G' \subset 2G$ resulta $o(G_1/2G_1) = 2$. De fato: Se $\bar{g} \in G_1$ então $\bar{g} = g + G'$ com $g \in G$ e assim, $\bar{g} = g_0 + 2h + G'$ com $h \in G$, e portanto $\bar{g} \in \bar{g}_0 + 2G_1$ ou $\bar{g} = 2h + G'$. No último caso $\bar{g} \in 2G_1$. Desde que $\bar{g}_0 \in 2G_1$ implica que $g_0 \in 2G$ (pois $\bar{g}_0 \in 2G_1 \Rightarrow \bar{g}_0 = 2(g + G') \Rightarrow g_0 + G' = 2g + G' \Rightarrow g_0 - 2g \in G' \subset 2G \Rightarrow g_0 \in 2G$) temos que $G_1 = 2G_1 \cup g_0 + 2G_1$. ∎

Examinemos um pouco mais os anéis $A(P,k)$ com o intuito de melhor esclarecer o leitor não familiarizado com esses anéis.

Como um anel de valorização convexo em relação a uma q-ordem é um subgrupo convexo do grupo aditivo $(F,+)$, obtemos por 2.3, que o conjunto de todos os anéis convexos em relação a uma q-ordem formam uma cadeia em relação a inclusão. Essa cadeia possui um "menor" elemento.

2.16 - PROPOSIÇÃO: *Sejam* $(F,P)$ *um corpo q-ordenado e* $A$ *um anel de* *valorização convexo em relação a* P. *Então* $A(P,Q) \subseteq A$.

DEMONSTRAÇÃO: Suponhamos que existe um anel de valorização $A$ de $F$, convexo relativamente a $P$ tal que $A \subsetneq A(P,Q)$. Seja $x \in A(P,Q)$ tal que $x \notin A$. Como $A$ é convexo em relação a $P$, $x > a$ para todo $a \in A$ e desde que $Q \subset A$, $x > q$ para todo $q \in Q$, o que é uma contradição. Logo, $A(P,Q) \subseteq A$. ∎

2.17 - PROPOSIÇÃO: *Sejam* $v$ *e* $w$ *valorização reais de um corpo q-ordenado* $(F,P)$.

*Se* $A_v \subset A_w$ *e* $v$ *é compatível com* $P$ *então* $w$ *é compatível com* $P$.

DEMONSTRAÇÃO: Sejam $a \in P$, e $w(a) < w(b)$. Então $w(ab^{-1}) < 0$ e $ab^{-1} \notin A_w$. Logo, $ab^{-1} \notin A_v$ e portanto $v(a) < v(b)$. Como $v$ é compatível com $P$, $a - b \in P$. ∎

Vejamos, agora, algumas observações básicas sobre extensões de valorizações necessárias ao contexto. Uma teoria mais completa pode ser encontrada em [E].

Seja $(F,v)$ um corpo valorizado e $K$ uma extensão de $F$. Dizemos que uma valorização $w$ de $K$ é uma *extensão* de $v$ (ou $w$ *estende* $v$) se $v = w_{|F}$ ou ainda, se o anel de valorização $B$ de $K$ associado a $w$ é uma extensão do anel de valorização $A$ de $F$ associado a $v$, isto é, se $A = B \cap F$. Nesse caso, diremos que $(K,w)$ é uma extensão de $(F,v)$. Por um resultado mostrado por Krull, sempre é possível estender $v$ (não necessariamente de modo único) a uma valorização $w$ de $K$. Por outro lado, é ime diato que toda valorização $w$ de $K$ estende exatamente uma valorização de $F$, precisamente $w|_F$ e que se $w$ estende $v$ então o grupo de valores $G_w$ de $w$ contém o grupo de valores $G_v$ de $v$, isto é, $G_v \subset G_w$.

Se $(K,w)$ for uma extensão de $(F,v)$ pode-se mostrar que para todo $0 \neq a \in K$, algébrico sobre $F$, existe $n \in \mathbb{Z}^{\cdot}$ tal que $n\, w(a) \in G_v$. Logo, se $K|F$ for uma extensão algébrica $G_w/G_v$ é um grupo de torção. Assim, sempre que $(K,w)|(F,v)$ for uma extensão algébrica $G_w \subset \bar{G}_v$ (fecho divisível de $G_v$).

Observemos ainda, que se $(K,w)$ for uma extensão de $(F,v)$ então a aplicação que a $x + M_v \in F_v$ associa $x + M_w \in K_w$ é um monomorfismo. Por isso, é natural identificar $F_v$ com sua imagem em $K_w$ e considerar $F_v \subset K_w$. Com essa identificação, se a extensão $(K,w) \mid (F,w)$ for algébrica então $K_w$ está contido no fecho algébrico de $F_v$, isto é, $K_w$ é uma extensão algébrica de $F_v$.

Lembramos ainda que se $K|F$ é uma extensão algébrica de corpos e $A_1$, $A_2$ são anéis de valorização que estendem o mesmo anel de $F$, então $A_1 \subset A_2$ implica em $A_1 = A_2$.

2.18 - PROPOSIÇÃO: *Sejam* $K|F$ *uma extensão algébrica de corpos e* $P$ *uma* q-*ordem de* $K$. *Então* $F$ *é cofinal em* $K$ *em relação a* $P$.

DEMONSTRAÇÃO: Temos $F \subset A(P,F) \subset K$. Além disso, $K$ e $A(P,F)$ são anéis de valorização de $K$ que estendem o mesmo anel de valorização de $F$ (precisamente $F$). Logo, como $A(P,F) \subset K$, $A(P,F) = K$, isto é, $F$ é cofinal em $K$. ∎

O Lema a seguir será usado na demonstração da Proposição 2.20.

2.19 - LEMA: *Sejam* F *um corpo*, A *um anel de valorização de* F *com ideal* M, k *um subcorpo de* F *maximal em relação a inclusão em* A *e a aplicação canônica* $\pi : A \to A/M$.

*O corpo de resíduos de* A *é uma extensão algébrica de* $\pi(k)$ *que é uma imagem isomorfa de* k.

DEMONSTRAÇÃO: Seja $t \in k$. $\pi(t) = t + M \in M$ se e somente se $t \in M$ e, portanto, se e somente se $t = 0$ pois $k \cap M = \{0\}$ (uma vez que k é corpo). Logo $\pi|_k$ é injetor e $\pi(k) \cong k$.

Seja $\alpha \in A$ tal que $\alpha \notin k$. Como k é maximal em relação à inclusão em A, $k(\alpha) \not\subset A$. Logo, existe $\beta \in k(\alpha)$ tal que $\beta \neq 0$ e $\beta \in M$. Sejam $f = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in k[x] \subset A_v[x]$ e $g = x^m + b_{m-1}x^{m-1} + \ldots + b_0 \in k[x] \subset A_v[x]$ tais que $\beta = f(\alpha).g(\alpha)^{-1}$. Como $v(\beta) = v(f(\alpha).g(\alpha)^{-1}) > 0$, $v(f(\alpha)) > v(g(\alpha)) \geq 0$. Assim $\pi(\alpha) = \alpha + M = \bar{\alpha}$ é raíz do polinômio $\bar{f} = x^n + \bar{a}_{n-1}x^{n-1} + \ldots + \bar{a}_0 \in \pi(k)[x] \cong k[x]$ e portanto A/M é extensão algébrica de $\pi(k)$. ∎

Identificando $\pi(k)$ com k podemos considerar A/M uma extensão algébrica de k.

2.20 - PROPOSIÇÃO: *Sejam* (F,P) *um corpo q-ordenado com* P *não arquimediana e* k *um subcorpo de* F. *Então:*

(i) k *é um subcorpo de* F *maximal em relação à inclusão em*

$A(P,k)$.

(ii) *O corpo de resíduos de* $A(P,k)$ *é uma extensão algébrica de* $\pi(k)$, *onde* $\pi$ *é a projeção canônica* $\pi : A(P,k) \to A(P,k)/M(P,k)$

(iii) *Com a ordem quociente* $\pi(k)$ *é cofinal no corpo de resíduos de* $A(P,k)$.

DEMONSTRAÇÃO:

(i) Suponhamos que existe um corpo $K$ tal que $k \subsetneq K \subset A(P,k)$. Seja $x \in K$ tal que $x \notin k$. Como $k$ é convexo em relação a $P$, $x - a \in P^{\cdot}$ para todo $a \in k$, contrariando $x \in A(P,k)$.

(ii) Como $k$ é um subcorpo de $F$ maximal em relação à inclusão em $A(P,k)$, o resultado decorre do Lema 2.19.

(iii) Decorre de (ii) e da Proposição 2.18.∎

Mostraremos, na proposição a seguir, que todo anel convexo em relação a uma q-ordem $P$ é do tipo $A(P,k)$ para algum subcorpo $k$ de $F$. Em 2.29 mostraremos que, se $A$ é um anel de valorização real de $F$, então existem uma q-ordem de $F$ e um subcorpo $k$ de $F$ tal que $A = A(P,k)$. Com isso, obtemos, em 2.30, um teorema demonstrado originalmente por Lang ([La]) usando o "Teorema da Extensão de Places Reais". A demonstração que daremos é devida a Prestel.

2.21 - PROPOSIÇÃO: *Sejam* $P$ *uma* q-*ordem de* $F$ *e* $A$ *um anel de va* *lorização de* $F$, *convexo em relação a* $P$. *Então, existe um subcorpo* $k$ *de* $F$ *tal que* $A = A(P,k)$.

DEMONSTRAÇÃO: A existência de subcorpos maximais de $k$ é garantida pelo Lema de Zorn, pois $Q \subset A$ uma vez que $A$ é convexo em relação a $P$. Seja então $k$ um subcorpo maximal de $F$ em relação à inclusão. Pelo Lema 2.19, $A/M_A$ é extensão algébrica de $\pi(k)$ onde $\pi$ é a projeção canônica $\pi : A \to A/M_A$. Assim, pela Proposição 2.18, $\pi(k)$ é cofinal em $A/M_A$ em relação à ordem $\bar{P} = (A \cap P)/M_A$. Seja $x \in A$. Então $x + M_A \in A/M_A$ e, portanto, existe $b \in k$ tal que $b + M_A - (x + M_A) = (b - x) + M_A \in \bar{P}$. Logo $x \in A(P,k)$ e, $A \subseteq A(k,P)$. Seja $x \in A(k,P)$. Então, existe $a \in k \subset A$ tal que $a - |x| \in P$ e, portanto, $x \in A$, pois $A$ é convexo em relação a $P$. Logo $A = A(k,P)$. ∎

Vamos estabelecer a seguir uma relação mais profunda entre q-ordens e valorizações reais. O resultado que veremos aprofunda a Proposição 2.10 ao mesmo tempo que estabelece uma recíproca de 2.11. E será um instrumento decisivo tanto na construção de exemplos de q-ordens próprias como na demonstração dos principais resultados que caracterizam os corpos que satisfazem a Lei de Sylvester Fraca. Mostraremos, em particular, que se $v$ é uma valorização real de $F$, pode-se obter uma q-ordem de $F$ compatível com $v$, a partir de uma q-ordem de $F_v$. Mas o resultado que apresentamos é mais geral. A demonstração é essencialmente técnica, com o grupo de valores de $v$ desempenhando papel importante.

Vejamos primeiro alguns conceitos auxiliares.

2.22 - DEFINIÇÃO: *Seja* $v : \dot{F} \to G$ *uma valorização de* $F$. *Uma q-secção de* $v$ *é uma aplicação* $s : G \to \dot{F}$ *que satisfaz:*

a) $v(s(g)) = g$ *para todo* $g \in G$, *isto é,* $s$ *faz corresponder a cada* $g \in G$ *um elemento de* $\dot{F}$ *cujo valor é* $g$.

b) $s(0) = 1$

c) $s(g_1 + g_2) \equiv s(g_1) \cdot s(g_2) \bmod \dot{F}^2$.

Pode-se verificar, facilmente, que para uma q-secção valem as propriedades:

$s(2g) \in \dot{F}^2$

$s(g_0 + 2g) \in s(g_0)\dot{F}^2$

$s(g_1) \equiv s(g_2) \bmod \dot{F}^2$ se e somente se $g_1 \equiv g_2 \bmod 2G$.

Existência de q-secção:

2.23 - PROPOSIÇÃO: *Para toda valorização* $v : \dot{F} \to G$ *existe uma q-secção de* $v$.

DEMONSTRAÇÃO: Consideremos a aplicação $s : G \to \dot{F}$ definida da seguinte maneira:

Para todo $g \in G$, colocamos $s(2g) = a^2$ onde $a$ é escolhido em $X_g = \{a \in \dot{F}$ tais que $v(a) = g\}$. Em particular, seja $s(0) = 1$.

Consideremos agora o $\mathbb{Z}/2\mathbb{Z}$-espaço vetorial $G/2G$. Seja $B$ um subconjunto de $G$ tal que $\{g + 2G;\ g \in B\}$ seja uma base de

$G/2G$. Para $g \in B$ colocamos $s(g) = a$, onde $a$ é escolhido no conjunto $X_g$. Como para todo $g \in G$, existem elementos $g_1, \ldots, g_n$ em $B$ tais que $\bar{g} = \bar{g}_1 + \ldots + \bar{g}_n$, ou seja, tais que $g = g_1 + \ldots + g_n + 2g'$ para algum $g' \in G$, podemos definir $s$ globalmente por $s(g) = s(g_1) \cdot s(g_2) \ldots s(g_n) . s(2g')$.

Mostremos que $s$ é uma q-secção de $v$:

a) $s$ está bem definida pois $\bar{g} \in G/2G$ se escreve de maneira única como combinação linear dos elementos da base.

b) $s(0) = 1$ por definição

c) $$v(s(g)) = v(s(g_1)) + \ldots + v(s(g_n)) + v(s(2g'))$$
$$= g_1 + \ldots + g_n + 2g'$$

d) Sejam $g, h \in G$. Temos:

$g = g_1 + \ldots + g_n + 2g'$ com $g_i \in B$ e $g' \in G$, e

$h = h_1 + \ldots + h_m + 2h'$ com $h_i \in B$ e $h' \in G$.

Suponhamos que $g_i = h_i$ para $1 \leq i \leq r = \min\{n, m\}$. Então $g + h = g_{r+1} + \ldots + g_n + h_{r+1} + \ldots + h_m + 2(g' + h' + g_1 + \ldots + g_r)$ e $s(g+h) = s(g_{r+1}) \cdot \ldots \cdot s(g_n) . s(h_{r+1}) \cdot \ldots \cdot s(h_m) . s(2g")$ onde $g" = g' + h' + g_1 + \ldots + g_r$. Logo $s(g+h) \cdot (s(h) \cdot s(g))^{-1} =$ $= [s(g_{r+1}) \cdot \ldots \cdot s(g_n) \cdot s(h_{r+1}) \cdot \ldots \cdot s(h_m) \cdot s(2g")] [(s(g_1) \cdot \ldots$ $\ldots s(g_r))^2 \cdot \ldots s(g_{r+1}) \cdot \ldots \cdot s(g_n) \cdot s(h_{r+1}) \cdot \ldots \cdot s(h_m) \cdot s(2g') \cdot$ $\cdot s(2h')]^{-1} = [s(2g")] [s(g_1) \cdot \ldots \cdot s(g_r)]^2 \cdot s(2g') \cdot s(2h')]^{-1} \in$ $\in \dot{F}^2$. Logo, $s(g + h) \equiv s(g) \cdot s(h) \mod \dot{F}^2$. ■

Uma q-secção $s : G \to \dot{F}$ para a qual vale a igualdade $s(g_1 + g_2) = s(g_1) \cdot s(g_2)$, para todo $g_1, g_2 \in G$, é chamada *secção* de v. Observemos que se $G \cong \mathbb{Z}$ e $v : \dot{F} \to G$ é uma valorização então podemos obter sempre uma secção de v. De fato: Seja $x \in F$ tal que $v(x) = 1$. Definimos $s : G \to \dot{F}$, $n \to x^n$. Assim definida, s é uma secção de v :

a) $s(0) = x^0 = 1$

b) $v(s(n)) = v(x^n) = n\, v(x) = n$

c) $s(n + m) = x^{n+m} = x^n . x^m = s(n).s(m)$.

Para facilitar a linguagem, analogamente à terminologia usada por Prestel em [P] (1973) passaremos a usar o termo *semi-ordem* de um corpo F para designar todo subconjunto S de F tal que $S + S \subset S$, $S \cap - S = \{0\}$ e $S \cup - S = F$. Se além disso, $S F^2 \subset S$, diremos que S é uma *semi-ordem quadrática*.

Observemos que uma semi-ordem de um corpo F é uma ordem do grupo aditivo (F,+) e que se F possui uma semi-ordem S compatível com a multiplicação ($S.S \subset S$) então S é uma ordem de F. Uma semi-ordem quadrática S tal que $1 \in S$ é uma q-ordem de F e sempre contém $\dot{F}^2$. Se $1 \notin S$ então $-1 \in S$ e assim $-F^2 \subset S$.

Um fato que usaremos mais adiante, que é fácil de ver, é que um corpo F com uma única ordem só pode ter duas semi-ordens quadráticas: $\Sigma F^2$ e $- \Sigma F^2$.

Visando simplificar a notação passaremos a representar:

a/b para indicar $ab^{-1}$ com $a \in F$ e $b \in \dot{F}$

e

[a] para indicar $a + M_v$ com $a \in A_v$.

2.24 - TEOREMA: *Sejam* $F$ *um corpo,* $v : \dot{F} \to G$ *uma valorização real de* $F$, $s$ *uma* $q$-*secção e* $\mathcal{P}$ *uma função de* $G$ *no conjunto das semi-ordens de* $F_v$ (isto é, *para cada* $g \in G, \mathcal{P}(g)$ *é uma semi-ordem de* $F_v$). $\mathcal{P}$ *induz em* $F$ *uma semi-ordem* $P$ *definida por:*

$$x \in P \leftrightarrow x = 0 \quad \text{ou} \quad [x/s(v(x)] \in \mathcal{P}(v(x))$$

*com as propriedades:*

a) Se $x \in P$ e $v(x) < v(y)$ então $x - y \in P$.

b) $1 \in P$ se e somente se $1 \in \mathcal{P}(0)$

c) $P$ *é uma semi-ordem quadrática se e somente se para todo* $g \in G$ *valem:*

(i) $\mathcal{P}(g)$ *é uma semi-ordem quadrática.*

(ii) $\mathcal{P}(g) = \mathcal{P}(g + 2h)$ *para todo* $h \in G$.

OBSERVAÇÕES:

1) Escolhendo-se a função $\mathcal{P}$ de modo que $1 \in \mathcal{P}(0)$ e que sejam válidos (i) e (ii) $P$ é uma q-ordem.

2) Se $P$ é uma q-ordem a propriedade a) estabelece a compatibilidade de $P$ com $v$.

3) A condição c) (ii) significa que a função $\mathcal{P}$ é constante nas classes laterais de $G$ módulo $2G$.

DEMONSTRAÇÃO DO TEOREMA: Vamos mostrar primeiro que $P$ é uma semi-ordem de $F$. a) $P + P \subset P$. De fato: Sejam $x, y \in P$. Podemos assumir $x \neq 0$ e $y \neq 0$ e aplicar a definição de $P$ a $x + y$. Consideremos dois casos.

1º Caso: $v(x) \neq v(y)$ e $v(x) < v(y)$. Então $v(x + y) = v(x)$ e $x + y/s(v(x + y)) = x/s(v(x)) + y/s(v(x))$. Assim $[x+y/s(v(x+y))] =$ $= [x/s(v(x))] + [y/s(v(x))]$. Como $v(y/s(v(x))) = v(y) - v(s(v(x))) =$ $v(y) - v(x) > 0$, temos que $[y/s(v(x))] = 0$. Logo $[x+y/s(v(x + y))] \in$ $\in \mathcal{P}(v(x)) = \mathcal{P}(v(x + y))$, pois $x \in P$ e portanto $x + y \in P$.

2º Caso: $v(x) = v(y)$. Assumindo $v(x + y) = v(x) = v(x)$ temos $x/s(v(x + y)) = x/s(v(x))$, $y/s(v(x + y)) = y/s(v(y))$ e, assim, como $\mathcal{P}(v(x)) = \mathcal{P}(v(y)) = \mathcal{P}(v(x + y))$, $[x + y/s(v(x + y))] \in \mathcal{P}(v(x+y))$.

A situação $v(x + y) > v(x) = v(y)$ não ocorre. De fato: Como por hipótese, $[x/s(v(x))] \in \mathcal{P}(v(x))$ e $[y/s(v(x))] = [y/s(v(y))] \in$ $\in \mathcal{P}(v(y)) = \mathcal{P}(v(x))$ temos que $[x + y/s(v(x))] = [x/s(v(x))] +$ $+ [y/s(v(x))] \in \mathcal{P}(v(x))$ e, portanto, $[x + y/s(v(x))] \neq 0$. Mas, então, $v(x + y/s(v(x))) = 0$ e $v(x + y) = v(s(v(x))) = v(x)$.

b) $P \cap -P = \{0\}$. De fato: $x \in P \cap -P$ implica em $x \in P$ e $-x \in P$. Logo se $x \neq 0$ então $[x/s(v(x))] \in \mathcal{P}(v(x))$ e $[-x/s(v(x))] \in$ $\in \mathcal{P}(v(x))$ ( $v(x) = -v(x)$! ), o que é uma contradição.

c) $P \cup -P = F$. De fato: se $x \in F$ e $x \neq 0$ então $[x/s(v(x))] \in$ $\in \mathcal{P}(v(x))$ ou $[-x/s(v(x))] \in \mathcal{P}(v(x)) = \mathcal{P}(v(-x))$ e portanto $x \in P$ ou $-x \in P$.

Vamos provar agora, que $P$ satisfaz as propriedades a) b) e c) do Teorema.

a) Se $v(x) < v(y)$ então $v(x - y) = v(x)$ e $x - y/s(v(x-y)) = x/s(v(x)) - y/s(v(x))$. Assim, $[x - y/s(v(x - y))] = [x/s(v(x))] - [y/s(v(x))]$. Como $v(y/s(v(x)) > 0$ temos que $[y/s(v(x))] = 0$. Logo, $[x - y/s(v(x - y))] \in \mathcal{P}(v(x - y))$ pois $x \in P$ e, portanto, $x - y \in P$.

b) $1 \in P \leftrightarrow 1 = [1/s(v(1))] \in \mathcal{P}(v(1)) = \mathcal{P}(0)$.

Para provar a propriedade c) vamos antes:

1) Provar que: Se $0 \neq [x] \in \mathcal{P}(g)$ então $s(g).x \in P$.

Como $v(s(g).x) = v(s(g)) = g$ temos $s(g)x/s(v(s(g).x)) = s(g)x/s(g) = x$. Logo $[s(g)x/s(v(s(g).x))] = [x] \in \mathcal{P}(g)$, resultando $s(g).x \in P$.

2) Observar que: $s(g_1 + g_2) = s(g_1).s(g_2) \bmod \dot{F}^2$ significa $s(g_1 + g_2) = s(g_1).s(g_2)t^2$ com $v(t) = 0$, pois se $s(g_1 + g_2) = s(g_1).s(g_2).t^2$ então $v(s(g_1 + g_2)) = v(s(g_1)) + v(s(g_2)) + v(t^2)$ e assim, $g_1 + g_2 = g_1 + g_2 + 2v(t)$ e $v(t) = 0$.

c) Suponhamos válidos (i) e (ii). Seja $x \in P$. Temos $[x/s(v(x))] \in \mathcal{P}(v(x)) = \mathcal{P}(v(x) + 2v(y)) = \mathcal{P}(v(xy^2))$. Além disso, para todo $y \in \dot{F}$ vale $[y^2/s(v(y^2))] \in \dot{F}_v^2$ e assim por (i), $[x/sv(x)] . [y^2/s(v(y^2))] = [xy^2/s(v(x).s(v(y^2))] \in \mathcal{P}(v(xy^2))$. Mas, então, novamente por (i), para $t \in U_v$ tal que $s(v(x)).s(v(y^2)) = s(v(x) + v(y2)).t^2$, vale $[t^{-2}]\,[xy^2/s(v(x) + v(y^2)) . t^2] = [xy^2/s(v(xy^2))] \in \mathcal{P}(v(xy^2))$. E, portanto, $xy^2 \in P$, isto é, $P$ é uma semi-ordem quadrática.

E, por último, é preciso provar que se $P$ é uma semi-ordem quadrática então valem (i) e (ii).

Sejam $\mathcal{P}(g)$ uma semi-ordem de $F_v$, $[x] \in \mathcal{P}(g)^{\bullet}$, $[y] \in F_v^{\bullet}$ e $z \in F^{\bullet}$ tal que $z = s(g)\, xy^2$. Como $v(s(g)x) = v(s(g)) = g$ temos $s(g).x/s(v(s(g).x)) = s(g).x/s(g) = x$. Logo $[s(g).x/s(v(s(g).x))] = [x] \in \mathcal{P}(g)$, resultando $s(g)x \in P$. Como $P$ é uma semi-ordem quadrática, $z = s(g).xy^2 \in P$ e, portanto, $[z/v(z)] \in \mathcal{P}(v(z))$. Finalmente, como $v(z) = v(s(g)xy^2) = g$ e $[xy^2] = [z/s(g)]$ temos $[x][y^2] = [xy^2] \in \mathcal{P}(g)$, ficando provada a condição (i).

Para provar (ii) sejam $g,h \in G$ e $[x] \in \mathcal{P}(g)^{\bullet}$. Temos $x.s(g) \in P$ e $s(2h) \in \dot{F}^2$. Como $P$ é quadrática $s(g).x.s(2h) \in P$. Assim, desde que $v(s(g).x.s(2h)) = g + 2h$ e $s(g + 2h) = s(g).s(2h).u^2$ com $u \in U_v$ temos $[s(g).x.s(2h)/s(g + 2h)] = [s(g).x.s(2h)/s(g).s(2h).u^2] = [x/u^2] \in \mathcal{P}(g + 2h)$. Como já provamos que $\mathcal{P}(g + 2h)$ é quadrática e $u \in U_v$, temos $[u^{-2}].[x/u^2] = [x] \in \mathcal{P}(g + 2h)$, isto é, $\mathcal{P}(g) \subset \mathcal{P}(g + 2h)$. Suponhamos que existe $[x] \in \mathcal{P}(g + 2h) \setminus \mathcal{P}(g)$. Então $[-x] \in \mathcal{P}(g) \subset \mathcal{P}(g + 2h)$, o que é uma contradição. Logo $\mathcal{P}(g) = \mathcal{P}(g + 2h)$. ■

Com as hipóteses e a notação do Teorema 2.24 temos:

2.25 - $P$ *é uma ordem se e somente se:*

1) $\mathcal{P}(0)$ é uma ordem

2) Para todo $g \in G$, $\mathcal{P}(g) = \mathcal{P}(0)$ ou $-\mathcal{P}(0)$

3) Para todo $g \in G$, $\mathcal{P}(g + 2h) = \mathcal{P}(g)$, qualquer que seja $h \in G$.

4) $$\mathcal{P}(g_1 + g_2) = \begin{cases} \mathcal{P}(0) & \text{se } \mathcal{P}(g_1) = \mathcal{P}(g_2) \\ -\mathcal{P}(0) & \text{se } \mathcal{P}(g_1) \neq \mathcal{P}(g_2) \end{cases}$$

De fato:

Suponhamos válidos 1) a 4) e sejam $x,y \in P^{\cdot}$ e $z \in U_v$ tal que $s(v(x) + v(y)) = s(v(x).s(v(y)).z^2$. Se $\mathcal{P}(v(x)) = \mathcal{P}(v(y)) = \mathcal{P}(0)$, temos $[x/s(v(x))]$, $[y/s(v(y))] \in \mathcal{P}(v(x)) = \mathcal{P}(0)$ e, portanto, $[xy/s(v(xy))] = [1/z^2].[x/s(v(x)].[y/s(v(y))] \in \mathcal{P}(0) = \mathcal{P}(v(x) + v(y)) = \mathcal{P}(v(xy))$. Logo $xy \in P$.

Se $\mathcal{P}(v(x)) = \mathcal{P}(v(y)) = -\mathcal{P}(0)$ também temos, desde que $\mathcal{P}(0)$ é uma ordem, que $[xy/s(v(xy))] \in \mathcal{P}(0) = \mathcal{P}(v(xy))$ e, portanto, $xy \in P$.

Se $\mathcal{P}(v(x) = P(0)$ e $\mathcal{P}(v(y) = -\mathcal{P}(0)$ (ou o contrário) temos $[xy/s(v(xy))] = [1/z^2].[x/s(v(x))].[y/s(v(y))] \in -\mathcal{P}(0) = \mathcal{P}(v(x)+v(y)) = \mathcal{P}(v(xy))$. E, portanto, $xy \in P$.

Mostraremos agora que se $P$ é uma ordem então valem 1) a 4).

1) $\mathcal{P}(0)$ é uma ordem.

$1 \in P$ implica em $[1/s(v(1))] = 1 \in \mathcal{P}(v(1)) = \mathcal{P}(0)$.

Sejam $[x] \in \mathcal{P}(0)$ e $[y] \in \mathcal{P}(0)$. Então $x.s(0) = x \in P$ e $y.s(0) = y \in P$. Mas então $xy \in P$ e, portanto, $[xy] = [xy/s(v(xy))] \in$ $\in P(v(xy)) = \mathcal{P}(0)$ ( $v(xy)=0!$ ).

2) Suponhamos que existe $g \in G$ tal que $\mathcal{P}(g) \neq \mathcal{P}(0)$ e $\mathcal{P}(g) \neq -\mathcal{P}(0)$. Sejam $x \in U_v$ e $y \in U_v$ tais que $[x] \in \mathcal{P}(g)$ e $[x] \in \mathcal{P}(0)$, $[y] \in \mathcal{P}(g)$ e $[y] \in -\mathcal{P}(0)$. Então $xs(g) \in P$, $x \in P$, $y.s(g) \in P$ e $-y \in P$, o que é uma contradição pois teríamos $s(g) \in P$ e $s(g) \in -P$, isto é, $s(g) = 0$.

3) Já foi provado em 2.24.

4) Suponhamos que existam $g_1, g_2 \in G$ tais que $\mathcal{P}(g_1) = \mathcal{P}(g_2) = \mathcal{P}(0)$ e que $\mathcal{P}(g_1 + g_2) = \mathcal{P}(0)$. Então, por 2, $\mathcal{P}(g_1 + g_2)$. $- \mathcal{P}(0)$.

Sejam $x \in P$ tal que $v(x) = g_1$ e $y \in P$ tal que $v(y) = g_2$. Então $[x/s(v(x))] \in \mathcal{P}(v(x)) = \mathcal{P}(g_1) = \mathcal{P}(0)$ e $[y/s(v(y))] \in \mathcal{P}(v(y)) = \mathcal{P}(g_2) = \mathcal{P}(0)$. Mas, então, $[xy/s(v(x)).s(v(y))] \in \mathcal{P}(g_1) = \mathcal{P}(g_2) = \mathcal{P}(0)$ e $[xy/s(v(x)+v(y)).z^2] \in \mathcal{P}(0)$, com $z \in U_v$ tal que $s(v(x).s(v(y)) = s(v(x) + v(y))z^2$. Assim, $[z^2][xy/s(v(x))+v(y))z^2] = [xy/s(v(xy))] \in$ $\in \mathcal{P}(0)$ e, portanto, $[xy/s(v(xy))] \notin -\mathcal{P}(0) = \mathcal{P}(g_1 + g_2) = \mathcal{P}(v(xy))$. Logo $xy \notin P$, o que é uma contradição. Se $\mathcal{P}(g_1) = \mathcal{P}(g_2) = -\mathcal{P}(0)$, temos, ainda assim, $[xy/s(v(x).s(v(y))] \in \mathcal{P}(0)$ e analogamente, chegamos à contradição $xy \notin P$.

Suponhamos, agora, que existam $g_1$, $g \in G$ tais que $\mathcal{P}(g_1) \neq \mathcal{P}(g_2)$ e $\mathcal{P}(g_1 + g_2) \neq -\mathcal{P}(0)$. Então $\mathcal{P}(g_1) = \mathcal{P}(0)$ e $\mathcal{P}(g_2) = -\mathcal{P}(0)$ (ou o contrário) e $\mathcal{P}(g_1 + g_2) = \mathcal{P}(0)$. Sejam $x, y \in P$ tais que $v(x) = g_1$, $v(y) = g_2$ e $z \in U_v$ tal que $s(v(x)+v(y)) = s(v(x))$ . $. s(v(y)).z^2$. Então $[x/s(v(x))] \in \mathcal{P}(0)$ e $[y/s(v(y))] \in -\mathcal{P}(0)$ e desde que $\mathcal{P}(0)$ é uma ordem $[xy/s(v(xy)] = [1/z^2][x/sv(x)][y/s(v(x)] \in$ $\in -\mathcal{P}(0)$. Portanto, $[xy/s(v(xy))] \notin \mathcal{P}(0) = \mathcal{P}(v(x)+v(y)) = \mathcal{P}(v(xy))$, isto é, $xy \notin P$. ∎

De 2.25 obtemos que um corpo F *admite q-ordens não arquimedianas se e somente se admite ordens não arquimedianas*. Basta observar que se F admite uma q-ordem P não arquimediana então $A(P,Q)$ é um anel convexo em relação a P e, portanto, a valorização associada a $A(P,Q)$ é uma valorização real. Por 2.25, existe, então, uma ordem de F compatível com v, a qual, por 2.12, é não arquimediana. Logo, como por 1.16, toda q-ordem arquimediana é uma ordem, *se F só possui ordens arquimedianas ... F não possui q-ordens próprias.*

Sejam, agora, P uma q-ordem de F, $v : F \to G$ uma valorização de F compatível com P e s uma q-secção de v. P induz uma aplicação $\mathcal{F}_P$ de G no conjunto das semi-ordens de $F_v$, onde para cada $g \in G$, $\mathcal{F}_P(g)$ é caracterizado por $[y] \in \mathcal{F}_P(g) \leftrightarrow$ $\leftrightarrow ys(g) \in P$, para todo $y \in U_v$.

Mostremos que a relação está bem definida, isto é, que ela independe da escolha dos representantes da classe residual:

Temos: $[x] = [y] \leftrightarrow x + M_v = y + M_v \leftrightarrow -x+y \in M_v \leftrightarrow (-x+y)y^{-1} \in$ $\in A_v$ (pois $y \in A_v \setminus M_v \Rightarrow y^{-1} \in A_v$) $\leftrightarrow (-x+y)y^{-1}s(g) \, . \, s(g)^{-1} \in M_v \leftrightarrow$ $\leftrightarrow v((-x + y)y{-}1 . s(g) \, . \, s(g^{-1})) > 0 \leftrightarrow v((-x + y).s(g)) - v(ys(g)) >$ $> 0 \leftrightarrow v(-x + y) \, s(g)) > v(ys(g))$. Logo, se $ys(g) \in P$, pela compatibilidade de v, $ys(g) - (-x + y)s(g) = xs(g) \in P$. Da mesma maneira mostra-se que se $x \, s(g) \in P$ então $y \, s(g) \in P$. Por outro lado, $\mathcal{F}_P(g)$ com $g \in G$ é uma semi-ordem de $F_v$.

Além disso, para todo $x \in \dot{F}$ temos $x \in P \leftrightarrow [x/s(v(x))] \in$ $\in \mathcal{F}_P(v(x))$.

Assim, existe uma correspondência bijetora entre o conjunto das q-ordens de F compatíveis com uma valorização v e o conjunto das funções $\mathcal{F}$ caracterizadas no Teorema 2.24. Isto é, acabamos de obter para q-ordens a recíproca do Teorema 2.24.

Observemos que uma ordem P de F é compatível com uma valorização real $v : \dot{F} \to G$ se e somente se a aplicação $\mathcal{F}_P$ satisfaz as condições 1) a 4) de 2.25.

Na verdade pode-se mostrar que:

2.26 - *A correspondência* $\mathcal{P} \to P$ *é uma bijeção entre o conjunto das funções* $\mathcal{P}$ *caracterizadas em* 2.24 *e o conjunto das* q-*ordens de* F *compatíveis com* v; *e induz uma bijeção entre o conjunto das funções* $\mathcal{P}$ *caracterizadas em* 2.25 *e o conjunto das ordens de* F *compatíveis com* v.

Estamos agora em condições de mostrar o resultado que caracteriza os corpos que satisfazem a Lei de Sylvester Fraca, como nos propusemos. É um resultado que nos permite, em muitos casos, concluir de maneira mais fácil a existência, ou não, de q-ordens próprias.

2.27 - TEOREMA: *Seja* F *um corpo formalmente real.*

$X_F = Y_F$ *se e somente se para toda valorização real* $v : \dot{F} \to G$

a) $o(G/2G) \leq 2$

b) *Se* $o(G/2G) = 2$ *então* $|X_{F_v}| = 1$.

DEMONSTRAÇÃO: Consideraremos primeiro uma valorização real $v : \dot{F} \to G$ para a qual (a) ou (b) é falso e construiremos uma q-ordem própria de F.

Se (a) é falso existem $g_1, g_2 \in G \setminus 2G$ tais que $g_1 - g_2 \notin 2G$. Sejam P uma ordem de $F_v$, $\mathcal{P}$ a aplicação de G no conjunto das semi-ordens de $F_v$ dada por:

$$\mathcal{P}(g) = \begin{cases} -P & \text{se } g \equiv g_1 + g_2 \mod 2G \\ P & \text{caso contrário} \end{cases}$$

e $s : G \to \dot{F}$ uma q-secção de $v$.

Pelo teorema 2.24, a aplicação $\mathcal{P}$ induz em $F$ uma q-ordem $P'$. Por 2.23, $P'$ é uma q-ordem própria de $F$ pois $\mathcal{P}(g_1)=\mathcal{P}(g_2)= = P$ e $\mathcal{P}(g_1 + g_2) = -P \neq \mathcal{P}(0)$, contradizendo $X_F = Y_F$. (não é difícil mostrar que $s(g_1) \in P'$, $s(g_2) \in P'$ e $s(g_1).s(g_2) \notin P'$, escolhendo $s$ convenientemente, de maneira que $s(g_1+ g_2)= s(g_1).s(g_2)$).

Se (b) é falso, $G = (g_0 + 2G) \cup 2G$ com $g_0 \notin 2G$ e $F_v$ possui pelo menos duas ordens distintas, $P$ e $P^*$. Sejam $s : G \to \dot{F}$ uma q-secção de $v$ e a aplicação $\mathcal{P}$ de $G$ no conjunto das semi-ordens de $F_v$ tal que:

$$\mathcal{P}(g) = \begin{cases} P & \text{se } g \in 2G \\ P^* & \text{se } g \in g_0 + 2G. \end{cases}$$

De modo análogo ao anterior $\mathcal{P}$ induz uma q-ordem $P'$ em $F$, que por 2.23, é própria, pois para $g \in g_0 + 2G$ temos $\mathcal{P}(g)\neq\mathcal{P}(0)$ e $\mathcal{P}(g) \neq -\mathcal{P}(0)$. (Pode-se mostrar que $s(g_0) \in P'$, $x \in P'$, onde $x \in U_v$ é tal que $[x] \in P$ e $[x] \in P^*$ e, no entanto, $x\,s(g_0) \in P'$.)

Suponhamos, agora, por hipótese, válidos a) e b). Seja $P$ uma q-ordem não arquimediana de $F$. Vamos mostrar que $P$ é uma ordem. Seja $v$ a valorização real associada ao anel $A(P,Q)$. Por hipótese, o grupo de valores $G$ de $v$ satisfaz: $o(G/2G) \leq 2$.

1º Caso: Se $o(G/2G) = 1$ então, por 2.8, $v$ é compatível com $P$, logo, por 2.24 $P$ é obtida através de uma função $\mathcal{P}$. Como $G = 2G$, $\mathcal{P}(g) = \mathcal{P}(0)$ para todo $g \in G$ e por 2.23, $P$ é uma ordem, uma vez que $\mathcal{P}(0)$ é a ordem quociente.

2º Caso: Se $o(G/2G) = 2$, pela Proposição 2.15, podemos considerar $v$ compatível com $P$. Então, por 2.24, $P$ é obtida através de uma função $\mathcal{P}$. Por hipótese, $F_v$ possui uma única ordem $\Sigma F_v^2$. Assim $\Sigma F_v^2$ e $-\Sigma F_v^2$ são as únicas semi-ordens quadráticas de $F_v$. Como $o(G/2G) = 2$ temos:

$$\mathcal{P}(g) = \begin{cases} \Sigma F_v^2 & \text{se } g \in 2G \\ \Sigma F_v^2 \text{ ou } -\Sigma F_v^2 & \text{se } g \notin 2G. \end{cases}$$

$\mathcal{P}$ satisfaz as condições 1) a 4) de 2.23. Os itens 1) a 3) são facilmente verificados. Mostremos o ítem 4): Sejam $g_1, g_2 \in G$. Suponhamos $g_1 \equiv g_2 \mod 2G$. Então $\mathcal{P}(g_1) = \mathcal{P}(g_2)$ e $\mathcal{P}(g_1 + g_2) = \Sigma F_v^2 = \mathcal{P}(0)$. Se $g_1 \not\equiv g_2 \mod 2G$ temos $g_1 \notin 2G$ e $g_2 \in 2G$ (ou o contrário) e, portanto $\mathcal{P}(g_2) = \Sigma F_v^2$ e $\mathcal{P}(g_1) = \mathcal{P}(g_1 + g_2) = \Sigma F_v^2 = \mathcal{P}(0)$ ou $\mathcal{P}(g_2) = \Sigma F_v^2$ e $\mathcal{P}(g_1) = \mathcal{P}(g_1 + g_2) = -\Sigma F_v^2 = -\mathcal{P}(0)$. Logo, $P$ é uma ordem. ∎

Esse teorema nos dá uma boa caracterização dos corpos que satisfazem $X_F = Y_F$, pois em muitos casos (a) e (b) são facilmente verificados. E será um instrumento decisivo no parágrafo de exemplos.

Para toda valorização $v : \dot{F} \to G$ introduzimos a notação:

$$X_F^v = \{P \in X_F;\ P \text{ é compatível com } v\}$$

$$Y_F^v = \{P \in Y_F;\ P \text{ é compatível com } v\}$$

Com raciocínio análogo à demonstração do Teorema 2.27 podemos provar o seguinte:

2.28 - TEOREMA: *Seja* $v : F \to G$ *uma valorização real de* $F$. *Então:*

$X_F^v = Y_F^v$ *se e somente se* $o(G/2G) \leq 2$ *e*

a) *se* $o(G/2G) = 2$ *então* $|X_{F_v}| = 1$

b) *se* $o(G/2G) = 1$ *então* $X_{F_v} = Y_{F_v}$ .

DEMONSTRAÇÃO: Se $o(G/2G) > 2$ ou $o(G/2G)=2$ e $|X_{F_v}| \neq 1$, como na demonstração de 2.27 obtemos uma q-ordem própria de $F$ cuja compatibilidade com $v$ pode ser verificada por 2.24.

Se $o(G/2G) = 1$ e $X_{F_v} \neq Y_{F_v}$, existe uma q-ordem própria $P_v$ de $F_v$. Seja $\mathcal{P}$ a aplicação constante $\mathcal{P} : G \to Y_{F_v}$ tal que $\mathcal{P}(g) = \mathcal{P}(0) = P_v$ para todo $g \in G$. Por 2.24 obtemos uma q-ordem de $P$ de $F$ compatível com $v$, a qual, por 2.25, é própria, pois $\mathcal{P}(0) = P_v$ não é uma ordem.

Vamos mostrar agora que tanto a) quanto b) implicam que $X_F^v = Y_F^v$.

Seja $P \in Y_F^v$ e $\mathcal{P}$ a função associada a $P$. Se $o(G/2G) = 1$ $\mathcal{P}(g) = \mathcal{P}(0)$ para todo $g \in G$. Por 2.22, $\mathcal{P}(0)$ é uma q-ordem e como $Y_{F_v} = Y_{F_v}$, $\mathcal{P}(0)$ é uma ordem. Logo, por 2.23, $P$ é uma ordem. Se $o(G/2G) = 2$ e $\Sigma F_v^2$ é a única ordem de $F_v$, obtemos como na demonstração anterior, que $P$ é uma ordem. E, portanto, $P \in X_F^v$.∎

O Teorema 2.27 nos permite também analisar com relativa facilidade o "going up" e o "going down" da Lei de Sylvester Fraca.

No § 3 desse capítulo apresentamos exemplos que mostram que a propriedade hereditária e o "going down" da L.S.F. nem sempre são válidos. O corpo $Q((x))$, por exemplo, satisfaz L.S.F. e $Q(\sqrt{2})((x))$ não satisfaz (Exemplo 2.52). Por outro lado, qualquer fecho real de $K = Q(\sqrt{2})((x))$ satisfaz a L.S.F. Porém, resultados que mostraremos a seguir estabelecem que, sob certas circunstâncias, a L.S.F. satisfaz o princípio de "going up" e de "going down".

Vamos mostrar, antes, usando 2.24, dois teoremas referentes a valorizações reais, os quais se farão necessários mais adiante, nesse trabalho.

2.29 - TEOREMA - *Sejam* $F$ *um corpo e* $A$ *um anel de valorização real de* $F$. *Então, existe uma q-ordem* $P$ *de* $F$ *e um subcorpo* $k$ *de* $F$ *tais que* $A = A(k,P)$.

DEMONSTRAÇÃO: Pelo Teorema 2.24, existe $P \in Y_F^v$. Por 2.6, $A$ é convexo em relação a $P$ e, pela Proposição 2.21, existe um subcorpo $k$ de $F$ tal que $A = A(k,P)$.∎

Observemos que, por 2.26, podemos garantir que existe $P \in X_F^v$ que satisfaz o Teorema.

O resultado a seguir responde a questão da extensão de valorizações reais de um corpo a extensões algébricas formalmente reais desse corpo.

2.30 - TEOREMA: *Seja* $v$ *uma valorização real de um corpo ordenado* $(F,P)$. *Então,* $v$ *se estende a uma valorização real do fecho real de* $(F,P)$ *se e somente se* $P \in X_F^v$. *Além disso, se* $v$ *se es-*

*tendo então essa extensão é única e o seu corpo de resíduos é isomorfo ao fecho real de* $(F_v, A_v \cap P/M_v) = (F_v, P_v)$.

DEMONSTRAÇÃO: $(\Rightarrow)$ Seja $(\bar{F},\bar{P})$ o fecho real de $(F,P)$ e $\bar{v}$ uma valorização real de $\bar{F}$. Então, como $\bar{F}$ tem ordem única e, por 2.25, $X_{\bar{F}}^{\bar{v}} \neq \emptyset$ temos que $\bar{P} \in X_{\bar{F}}^{\bar{v}}$. Logo, $A_{\bar{v}}$ é convexo relativamente a $\bar{P}$ e, portanto, $A_v = A_{\bar{v}} \cap F$ é convexo em relação a $P$. E, por 2.6, $P \in X_F^v$. Para mostrar que, caso $v$ se estenda a $(\bar{F},\bar{P})$ então essa extensão é única, suponhamos que $v_1$ seja outra valorização real de $\bar{F}$ tal que $A_{v_1} \cap F = A_v$. Então $v_1$ é compatível com a única ordem de $\bar{F}$, isto é, $\bar{P} \in X_{\bar{F}}^{v_1}$. Mas,então, $A_{v_1}$ é convexo relativamente a ordem $\bar{P}$. Assim, $A_{v_1} \subset A_{\bar{v}}$ ou $A_{\bar{v}} \subset A_{v_1}$ e, como $A_{v_1}$ e $A_{\bar{v}}$ estendem o mesmo anel de valorização de $F$ e $\bar{F}|F$ é uma extensão algébrica, $A_{v_1} = A_{\bar{v}}$ e, portanto, $v_1$ e $\bar{v}$ são equivalentes.

$(\Leftarrow)$ Suponhamos que $P \in X_F^v$. Então, $A_v$ é convexo em relação a $P$ e, por 2.21, existe um subcorpo $k$ de $F$ tal que $A_v = A(k,P)$. O anel $A(k,\bar{P}) \subset \bar{F}$ estende o anel $A_v$. Assim, se $\bar{v}$ é a valorização associada a $A(k,\bar{P})$, então $\bar{v}$ é uma valorização real de $\bar{F}$ que estende $v$.

Agora, seja $(\bar{k}, \overline{\bar{P} \cap k})$ o fecho real de $(k, P \cap k)$ contido em $\bar{F}$. Então, $\bar{k}$ é real fechado e $k$ é cofinal em $\bar{k}$ (pois $\bar{k}|k$ é uma extensão algébrica). Logo, $\bar{k} \subset A_{\bar{v}}$.Sejam, $P_{\bar{v}} = A_{\bar{v}} \cap \bar{P}/M_{\bar{v}}$ e $\bar{\pi}$ a aplicação canônica $\bar{\pi} : A_{\bar{v}} \to A_{\bar{v}}/M_{\bar{v}} = \bar{F}_{\bar{v}}$. Logo, $\bar{\bar{\pi}}(k) \simeq k$ e $(\bar{\pi}(\bar{k}), P_{\bar{v}} \cap \bar{\pi}(\bar{k}))$ é um subcorpo real fechado de $(\bar{F}_{\bar{v}}, \bar{P}_{\bar{v}})$. Por 2.19, $F_v$ é uma extensão algébrica de $\pi(k)$. Além disso, $\bar{F}_{\bar{v}}$ é extensão algébrica de $F_V$. Assim $\bar{F}_{\bar{V}}$ é extensão algébrica de $\pi(k)$. Como $k \subset \bar{k}$ e $\bar{\pi}$ estende $\pi$, concluimos que $(\bar{F}_{\bar{V}}, P_{\bar{V}})$ é uma extensão algébrica ordenada de $(\bar{\pi}(\bar{k}), P_{\bar{V}} \cap \bar{\pi}(\bar{k}))$. Logo, $(\bar{F}_{\bar{V}}, P_{\bar{V}})$ é o fecho real de $(F_V, P_V)$. ∎

No Teorema 2.33 tem importância os corpos hereditariamente euclideanos. Daremos agora, apenas as noções necessárias à demonstração da proposição. No Capítulo IV serão dados mais resultados sobre essa classe de corpos.

2.31 - DEFINIÇÃO:

a) *Um corpo* F *é euclideano se é formalmente real e para* $x \in \dot{F}$, $x \in F^2$ *ou* $-x \in F^2$. *Isto é,* F *é euclideano se e somente se* $F^2$ *é um cone positivo de* F.

b) *Um corpo* F *é hereditariamente euclideano* (notação: h.e) *se* F *e toda extensão algébrica formalmente real de* F *são euclideanos.*

Os corpos euclideanos são precisamente os corpos pitagóricos com uma única ordem. Como exemplo de corpos h. e. temos os corpos reais fechados, com os quais os corpos h. e. possuem muitas propriedades em comum. Estes não são, no entanto, os únicos exemplos.

É imediato que F é h.e. se e somente se F e toda extensão algébrica f.r. de F admitem uma única ordem. Num sentido, a afirmação é trivial. Para prová-la no outro sentido basta considerar que, se K é uma extensão algébrica f.r de F e K não é euclideano, então existe uma ordem $P$ de $K$ e um elemento $a \in P^{\cdot}$ tal que $a \notin K^2$. E, portanto, por 1.8, $K(\sqrt{a})$ admite pelo menos duas ordens. Como $K(\sqrt{a})$ é uma extensão algébrica de $F$ temos uma contradição.

Para demonstrar o Teorema 2.33 necessitamos também do seguinte lema:

2.32 - LEMA: *Seja* $H$ *um grupo abeliano ordenado e* $G$ *um subgrupo de* $H$ *tal que* $o(H/G) < \infty$ *.Então:*

(i) $o(G/2G) = 1 \Rightarrow o(H/2H) = 1$

(ii) $o(G/2G) = 2 \Rightarrow o(H/2H) = 2$

DEMONSTRAÇÃO:

(i) Sejam $h \in H$, $m \in \mathbb{N}$ e $g \in G$ tais que $o(h + G) = m$ e $mh = 2g$. Suponhamos que $m$ é par. Então $m = 2n$ para algum $n \in \mathbb{N}$ e $2(nh - g) = 0$. Como $H$ é livre de torção ($H$ é ordenado!) $nh - g = 0$ e, portanto, $nh = g$, contrariando $o(h+G)=m$. Logo, $m = 2k - 1$ com $k \in \mathbb{N}^{\cdot}$. Mas, então, $(2k-1)h = 2g$ e assim $h = 2(kh - g) \in 2H$.

(ii) Seja $G = 2G \cup g_0 + 2G$. Podemos ter: $g_0 \notin 2H$ ou $g_0 \in 2H$.

Suponhamos, primeiro, que $g_0 \notin 2H$ e seja $h \in H$. Se $o(h + G)= 2k$ então $2kh = g_0 + 2g$ com $g \in G$ pois $2kh = 2g$ implica em $kh = g$, o que contraria $o(h + g) = 2k$. Logo $g_0=2(kh-g)\in 2H$. Mas isso contradiz a suposição $g_0 \notin 2H$ e portanto $o(h + G) = 2k + 1$. Então

$(2k+1)h = 2g$ e, nesse caso, $h \in 2H$ ou $(2k+1)h = g_0 + 2g$ e nesse caso $h \in g_0 + 2H$. Assim, $H = 2H \cup g_0 + 2H$, isto é, $o(H/2H) = 2$.

Suponhamos, agora, que $g_0 \in 2H$ e seja $A = \{n \in \mathbb{N};$ para todo $0 \leq i \leq n$ existe $h_i \in H$ com $2^i h_i \in g_0 + 2G\}$. $A \neq \emptyset$ pois $0 \in A$ uma vez que $2^0 g_0 \in g_0 + 2G$. Se $n \in A$ temos $h_i + G \neq$ $\neq h_j + G$ para todo $0 \leq i, j \leq n$ tais que $i \neq j$ (pois $h_i = h_j + g$ com $g \in G$ e $1 < j$ $\Rightarrow 2^j h_i = 2^j h_j + 2^j g \Rightarrow 2^{j-i}(2^i h_i) = 2^j h_j + 2^j g \Rightarrow$ $\Rightarrow$ existem $g_i, g_j \in G$ tais que $2^{j-i}(g_0 + 2g_i) = g_0 + 2g_j + 2^j g \Rightarrow$ $\Rightarrow g_0 \in 2G$ - o que é uma contradição). Logo, qualquer que seja $n \in A, n \leq o(H/G)$. Para todo $n \in A$, $o(h_n + G) = 2^n$ pois de $2^n h_n \in$ $\in g_0 + 2G$ obtemos que $o(h_n + G) \mid 2^n$ e, portanto, $o(h_n + G) = 2^m$ com $m \leq n$. Se $m < n$ então existe $g \in G$ tal que $2^m h_n = g$ e $2^{n-m} g = 2^{n-m}\, 2^m h_n = 2^n h_n = g_0 + 2g_n$, isto é, $g_0 \in 2G$ - o que é uma contradição. Logo $m = n$, isto é, $o(h_n + G) = 2^n$. Seja $n = \text{máx}.A$. Então $h_n \notin 2H$ pois, se $h_n = 2h$ de $2^n h_n = g_0 + 2g$ obtemos $2^{n+1} h = g_0 + 2g$, contrariando a maximalidade de $n$.

Seja $I = \{r \in \mathbb{N}^{*};\ \exists h \in H$ com $o(h + G) = 2^r$ e $h + G \notin$ $\in [h_n + G] \subset H/G\}$. Suponhamos que $I \neq \emptyset$, isto é, que existem $r \in \mathbb{N}$ e $h \in H$ tais que $o(h+G) = 2^r$ e $h + G \notin [h_n + G]$. Seja $r =$ $= \min I$. Então, $2^r h = g_0 + 2g$ com $g \in G$ e, portanto, $r \leq n$. Temos $2^r h - 2g = g_0 = 2^n h_n - 2g_n$ com $g_n \in G$, isto é, $2^{r-1} h - g = 2^{n-1} h_n - g_n$ e $2^{r-1}(h - 2^{n-r} h_n) = g - g_n$. Logo, $o(h - 2^{n-r} h_n) \mid 2^{r-1}$ e, portanto, $o(h - 2^{n-r} h_n) = 2^s$ com $s \leq r - 1$. Mas, então, $s \notin I$ e $(h - 2^{n-r} h_n) + G \in$ $\in [h_n + G]$, isto é, existe $t \in \mathbb{N}$ tal que $(h - 2^{n-r} h_n) + G = t(h_n + G)$ e, consequentemente, $h + G = (t + 2^{n-r}) h_n + G \in [h_n + G]$, o que é uma contradição. Logo $I = \emptyset$.

Temos que $o(H/2H) \geq 2$ pois se $H = 2H$ então para todo $i \geq 0$ existe $h_i \in H$ tal que $g_0 = 2^i h_i$, contrariando $n \leq o(H/G)$ para $n \in A$.

Seja $h \in H$.

a) Se $o(h + G) = 2k + 1$ então $(2k + 1)h = 2g$ com $g \in G$ e, portanto, $h = 2g - 2kh \in 2H$ ou $(2k + 1)h = g_0 + 2g$ com $g \in G$ e, portanto, $h = g_0 + 2g - 2kh \in 2H$.

b) Se $o(h + G) = 2^r$ então $r \leq n$ e, portanto, existe $s \in \mathbb{N}$ tal que $h + G = s(h_n + G)$. Logo, $h = sh_n + 2g$ ou $h = sh_n + g_0 + 2g$. Se $s = 2t$, então $h = 2(th_n + g) \in 2H$ ou $h = g_0 + 2(th_n + g) \in g_0 + 2H = 2H$. Se $s = 2t + 1$, então $h = h_n + 2(th_n + g) \in h_n + 2H$ ou $h = h_n + g_0 + 2(th_n + g) \in h_n + 2H$.

c) Se $o(h + G) = 2^r m$ com $(2,m) = 1$ então existem, $a, b \in \mathbb{Z}$ tais que $2^r a + mb = 1$ e $h = 2^r ah + mbh$. Como $2^r(mbh + G) \subset G$, $o(mbh + G) \mid 2^r$ e, portanto, $o(mbh + G) = 2^s$ com $s \leq r$. Então, $mbh \in 2H$ e, portanto, $h = 2^r ah + mbh \in 2H$ ou $mbh \in h_n + 2H$ e, portanto, $h = 2^r ah + mbh \in h_n + 2H$.

Logo, $H = 2H \cup h_n + 2H$ e $o(H/2H) = 2$.

Voltemos aos corpos [illegible]. Pelo Lema, é imediato que um corpo euclideano e todas as suas extensões algébricas finitas (e, em consequência, também as infinitas - veja a demonstração de 2.33) não possuem q-ordens próprias, isto é, satisfazem a L.S.F.. Pois, para todo $x \in \dot{F}$ temos $x \in \dot{F}^2$ ou $-x \in \dot{F}^2$. Assim, se $v : \dot{F} \to G$ é uma valorização real de $F$, então $v(x) = v(y^2) = 2v(g)$, para algum $y \in \dot{F}$ e, portanto, $o(G/2G) = 1$.

Logo, os corpos h.e. são um primeiro exemplo onde a L.S.F. é hereditária.

No Teorema 2.33 vemos que todos os corpos que satisfazem a L.S.F. tem relação com os corpos h.e.

2.33 - TEOREMA (*Hereditariedade da* L.S.F.): *Seja* F *um corpo. Toda extensão algébrica de* F *satisfaz a* L.S.F. *se e somente se para toda valorização real* $v : \dot{F} \to G$, $o(G/2G) \leq 2$ *e se* $o(G/2G) = 2$ *então* $F_v$ *é hereditariamente euclideano.*

DEMONSTRAÇÃO: Sejam K uma extensão algébrica infinita de F tal que $X_K \neq Y_K$, e P uma q-ordem própria de K. Existem $a,b \in K$ tais que a,b e $-ab \in P$. $P \cap F(a,b)$ é, então, uma q-ordem própria de F(a,b) que é extensão finita de F. Portanto, podemos nos restringir ao caso em que K é uma extensão finita de F.

Se F não possui valorizações reais então F só possui ordens arquimedianas e, portanto, F e toda extensão algébrica de F não possuem q-ordem própria. E, o resultado vale.

Admitamos então a existência de valorizações reais e suponhamos que a L.S.F. é válida para toda extensão algébrica finita de F. Por absurdo, vamos supor que $v : \dot{F} \to G$ é uma valorização real com $o(G/2G) = 2$, que $L|F_v$ é uma extensão algébrica e que L possui mais de uma ordem. Existe uma extensão (E,v',G) de (F,v,G), algébrica, cujo corpo de resíduos é L ([E], Teorema 27.1). Como L é f.r., E é f.r. e v' é uma valorização real.

Por hipótese, $E$ satisfaz L.S.F., o que, pelo Teorema 2.27, é uma contradição pois $E_{V'} = L$ (que possui mais de uma ordem) e $o(G/2G)=2$.

Reciprocamente, sejam $K$ uma extensão finita de $F$, $w : K^{\cdot} \to G_w$ uma valorização real e $v = w_{|F}$. Então, $[K_w : F_v] < \infty$ e $o(G_w/G_v) < \infty$ (ver [E] Corolário 13.10). Como $X_F = Y_F$, $o(G_v/2G_v) \leq$ $\leq 2$. Logo, pelo Lema 2.32, $o(G_w/2G_w) \leq 2$. Desde que $[K_w:F_v] < \infty$ e $w$ é uma valorização real, $K_w|F_v$ é uma extensão algébrica f.r. e, portanto, como $F_v$ é h.e., $|X_{K_w}| = 1$. Assim, pelo Teorema 2.27, $X_K = Y_K$. ■

2.34 - COROLÁRIO:

a) *Seja* $K|F$ *uma extensão algébrica de corpos. Se para toda valorização real* $v : \dot{F} \to G$, $o(G/2G) = 1$ *então* $X_K = Y_K$.

b) *Se* $F$ *é um corpo com uma única ordem então toda extensão algébrica* $K$ *de* $F$ *satisfaz* $X_K = Y_K$.

c) *Se* $F$ *é um corpo que admite apenas ordens arquimedianas então toda extensão algébrica* $K$ *de* $F$ *satisfaz* $X_K = Y_K$.

DEMONSTRAÇÃO:

a) Consequência imediata do Teorema.

b) Se a ordem é arquimediana o resultado é imediato.

Suponhamos, então, que a ordem é não arquimediana. Vamos mostrar que o grupo de valores de toda valorização real $v : \dot{F} \to G$ de $F$ é 2-divisível: Sejam $g \in G$ e $x \in F^{\cdot}$ tais que $v(x) = g$.

Como $v(-x) = v(x)$ podemos supor $x$ positivo. Por 1.6, $x = x_1^2 + \ldots + x_n^2$ com $x_1, x_2, \ldots, x_n \in F$. Suponhamos que $v(x) > \{\min v(x_1^2), \ldots, v(x_n^2)\} = v(x_j^2)$ para $j \in \{1,\ldots,n\}$. Então $\frac{x}{x_j^2}, \sum_{\substack{i=1 \\ i \neq j}}^{n} (\frac{x_i}{x_j})^2 \in M_v$ e como $\frac{x}{x_j^2} = 1 + \sum_{\substack{i=i \\ i \neq j}}^{n} (\frac{x_i}{x_j})^2$ teríamos $0 = [\frac{x}{x_j^2}] = [1] + \sum_{i=1}^{n} [\frac{x_i}{x_j}]^2$, o que é uma contradição com a condição de $F_v$ ser formalmente real. Logo, $g = v(x) = \min \{v(x_1^2), \ldots, v(x_n^2)\} = 2v(x_j) \in 2G$ e $o(G/2G) = 1$. E pela letra a) o resultado segue .

c) Basta observar que $F$ não possui valorização real e aplicar o Teorema 2.33. Se $F$ possuísse valorização real $v$ existiria em $F$ uma ordem compatível com $v$, que por 2.12 seria não arquimediana. ■

Na letra c) do Corolário provamos novamente que todo corpo de números algébricos satisfaz a L.S.F..

2.35 - PROPOSIÇÃO (going down): *Seja* $K|F$ *uma extensão de corpos. Se toda* q-*ordem de* $F$ *se estende a* $K$ *e* $X_K = Y_K$ *então* $X_F = Y_F$.

DEMONSTRAÇÃO: Seja $P$ uma q-ordem de $F$. Por hipótese, $P$ se estende a uma q-ordem $P_K$ de $K$. Como $X_K = Y_K$, $P_K$ é uma ordem e , portanto, $P_K \cap F = P$ é uma ordem. ■

Usando o Lema 2.36, vamos obter em 2.37 um Corolário dessa proposição.

2.36 - LEMA: *Seja* $K|F$ *uma extensão de corpos. Uma q-ordem* $P$ *de* $F$ *se estende a uma q-ordem de* $K$ *se e somente se* $\sum_{i=1}^{n} a_i x_i^2 = 0$ *com* $n \in \mathbb{N}$ *e* $a_i \in P^{\cdot}$ *só possui solução trivial em* $K$ *(ou, se e somente se toda forma quadrática* $< a_1, \ldots, a_n >$ *com* $a_i \in F^{\cdot}$ *definida em relação a* $P$ *é anisotrópica em* $K$ *).*

DEMONSTRAÇÃO: É imediato que se $P$ se estende a $K$ a única solução de $\sum_{i=1}^{n} a_i x_i^2 = 0$ em $K$ é a trivial.

Para mostrar a recíproca seja $P_0 = \{ \sum_{i=1}^{n} a_i x_i^2,\ a_i \in P^{\cdot}$ e $x_i \in K\}$. É fácil verificar que $P_0 + P_0 \subset P_0$ e $y^2 P_0 \subset P_0$ para todo $y \in K$. Seja $z \in P_0 \cap -P_0$ tal que $z \neq 0$ isto é, $z = \sum_{i=1}^{n} a_i \alpha_i^2$ com $a_i \in P^{\cdot}$, $\alpha_i \in K$ e $\alpha_i \neq 0$ para algum $i \in \{1, \ldots, n\}$ e $z = - \sum_{j=1}^{n} b_j \beta_j^2$ com $b_j \in P^{\cdot}, \beta_j \in K$ e $\beta_j \neq 0$ para algum $j \in \{1, 2, \ldots, n\}$. Então $\sum_{i=1}^{n} a_i \alpha_i^2 + \sum_{j=1}^{n} b_i \beta_j^2 = 0$ possui solução não trivial, o que contraria a hipótese. Logo, $P_0 \cap -P_0 = \{0\}$ e, portanto, $P_0$ é um pré-q-cone de $K$, que, como $1 \in P_0$ pode ser estendido a um q-cone $P'$ de $K$. $P'$ é uma q-ordem de $K$ que estende $P$. ∎

Observemos que se $P$ for uma ordem, então $P_0 . P_0 \subset P_0$ e a extensão de $P$ à $K$ é uma ordem.

2.37 - COROLÁRIO:

a) *Seja* $F$ *uma extensão finita de* $F$, f.r. *e de grau ím-*

*Se* $X_K = Y_K$ *então* $X_F = Y_F$.

b) *Seja* $K = F(\sqrt{a})$ *onde* $a \in \Sigma F^{\cdot 2}$. *Se* $X_K = Y_K$ *então* $X_F = Y_F$.

c) *Seja* $F_P$ *o fecho pitagórico (="menor" corpo pitagórico que contém* F) *de* F. *Se* $X_{F_P} = Y_{F_P}$ *então* $X_F = Y_F$.

OBSERVAÇÃO: O fecho pitagórico de um corpo $F$ é a intersecção da família $\{F_i\}$ de todos os corpos pitagóricos contidos no fecho algébrico de $F$ e pode ser obtido pela "composição" de todos os corpos $K$ para os quais existe uma cadeia de corpos $F = K_0 \subset K_1 \subset \subset \ldots \subset K_m = K$ com $K_{i+1} = K_i(\sqrt{1+\alpha_i^2})$ e $\alpha_i \in K_i$.

DEMONSTRAÇÃO:

a) Seja $P$ uma q-ordem de F. Suponhamos que a equação $\sum_{i=1}^{n} a_i x_i^2 = 0$ com $a_i \in P^{\cdot}$ possua solução não trivial em K. Então, como o grau da extensão é ímpar pelo Teorema de Springer ([L] Capítulo VII - Teorema 2.3), $\sum_{i=1}^{n} a_i x_i^2 = 0$ possui solução não trivial em F, contrariando $a_i \in P^{\cdot}$. Portanto, a equação $\sum_{i=1}^{n} a_i x_i^2 = 0$ só possui solução trivial em $K$ e, assim, pelo Lema 2.33, P se estende a uma q-ordem $P_K$ de K. Como $X_K = Y_K$, pela proposição , $X_F = Y_F$.

b) Seja $P$ uma q-ordem de $F$ e a equação $\sum_{i=1}^{n} a_i x_i^2 = 0$ com $a_i \in P^{\cdot}$. Suponhamos que $\sum_{i=1}^{n} a_i (b_i + c_i\sqrt{a})^2 = 0$ com $b_i, c_i \in F$. Então $\sum_{i=1}^{n} a_i(b_i^2 + 2b_ic_i\sqrt{a} + ac_i^2) = 0$ e $\Sigma b_i^2 + ac_i^2 = 0$. Como $aP \subset P$ temos $b_i^2 + ac_i^2 \in P$ para todo $1 \leq i \leq n$. Portanto $b_i^2 = ac_i^2 = 0$ e $b_i = c_i = 0$. Logo, $\sum_{i=1}^{n} a_ix_i^2 = 0$ só possui solução trivial em K e P se estende a uma q-ordem $P_K$ de K. Como $X_K = Y_K$, pela proposição, $X_F = Y_F$.

c) Basta observar que, conforme mostramos em b), toda q-ordem de um corpo K se estende a $K(\sqrt{1+\alpha^2})$ com $\alpha \in K$. ■

Com o Lema 2.36, podemos também mostrar facilmente um resultado bem conhecido da teoria de corpos formalmente reais.

2.38 - PROPOSIÇÃO: *Seja* $K|F$ *uma extensão finita de corpos. Se* $|X_K| = 1$ *então* $|X_F| = 1$.

DEMONSTRAÇÃO: Sejam P a única ordem de K, $(\bar{K},\bar{P})$ o fecho real de $(K,P)$, $K = F(\alpha)$ e $f \in F[x]$ o polinômio minimal de $\alpha$ sobre F. Como o número de raízes de f em $\bar{K}$ coincide com o número de ordens de K ([R] Capítulo IX Teorema 10), f possui uma única raiz em $\bar{K}$. Então, por 1.10 (i) f se decompõe em $\bar{K}$ em um só fator linear e em fatores quadráticos e, portanto, $\partial f = [K : F]$ é ímpar.

Seja, agora, uma ordem $P_1$ de F e a equação $\sum_{i=1}^{n} a_ix_i^2 = 0$ com $a_i \in P_1^{\cdot}$. Pelo Lema de Springer $\sum_{i=1}^{n} a_ix_i^2 = 0$ só possui solução trivial em K e, por 2.36, $P_1$ se estende a uma ordem de

K. Logo, toda ordem de $F$ se estende a $K$ e, portanto, $P \cap F$ é a única ordem de $F$. ∎

2.39 - COROLÁRIO: *Se $K|F$ é uma extensão finita de corpos e $K$ é euclideano então $F$ é euclideano.*

DEMONSTRAÇÃO: Basta observar que se $o(K/\dot{K}^2) = 2$ e $[K:F]$ é ímpar então $o(F/\dot{F}^2) = 2$. ∎

Dentro do estudo do "going up" e "going down" a Lei de Sylvester Fraca relaciona fortemente um corpo com o seu fecho pitagórico, conforme mostramos na proposição abaixo. Nessa proposição, usaremos a expressão "extensão admissível de $F$" para nos referirmos a um corpo $K$ de $F$ para o qual existe uma cadeia de corpos $F = K_0 \subset K_1 \subset \ldots \subset K_m = K$ tais que, para todo $0 \leq i < m$, $K_{i+1} = K_i(\sqrt{\alpha})$ com $\alpha \in \Sigma K_i^2$.

2.40 - PROPOSIÇÃO: Seja $F$ um corpo. São equivalentes:

(1) $F_p$ *satisfaz* L.S.F.

(2) *Para toda valorização real* $v : F \to G$

a) $o(G/2G) \leq 2$ e

b) se $o(G/2G) = 2$ então $F_v$ é euclideano

(3) $F(\sqrt{t})$ *satisfaz a* L.S.F. *para todo* $z \in F$, *totalmente positivo.*

(4) *Toda extensão admissível* $K$ *de* $F$ *satisfaz a* L.S.F..

DEMONSTRAÇÃO:

(1) $\Rightarrow$ (3) Para todo $t \in F$, totalmente positivo, $F(\sqrt{t}) \subset F_p$. Logo por 2.37 (c), $F(\sqrt{t})$ satisfaz a L.S.F..

(3) $\Rightarrow$ (2) Seja $v : F \to G$ uma valorização real de $F$. Como, por 2.37 (c), $F$ satisfaz L.S.F., temos que $o(G/2G) \leq 2$ e se $o(G/2G) = 2$ então $|X_{F_v}| = 1$. Logo, basta provar que se $o(G/2G)=2$ então $F_v$ é euclideano. Seja $a \in U_v$ tal que $\bar{a}$ é um elemento positivo em $F_{\bar{v}}$. Suponhamos que $\bar{a} \notin F_v^2$. Como $\bar{a} = \sum_{i=1}^{n} \bar{a}_i^2$ com $\bar{a}_i \in F_v$ e podemos assumir $a = \sum_{i=1}^{n} a_i$ com $a_i \in F$. Sejam $K = F(\sqrt{a})$ e $w : K \to G_w$ uma valorização real que estende $v$. Então $K_w \supset F_v(\sqrt{\bar{a}})$ e, portanto, $[K_w : F_v] \geq 2$. Como $[K : F] = 2$, por [E] Corolário 17.5 , $G \simeq G_w$ , $w$ é a única extensão de $v$ a $K$ e $K_w = F_v(\sqrt{\bar{a}})$. Como $F_v(\sqrt{\bar{a}})$ tem duas ordens e $o(G_w/2G_w) = 2$, por 2.27, $K = F(\sqrt{a})$ não satisfaz a L.S.F. o que é uma contradição com (2). Logo $\bar{a} \in F_v^2$ e $F_v$ é euclideano.

(2) $\Rightarrow$ (4) Basta mostrar que se um corpo $F$ satisfaz (2) então $F(\sqrt{t})$ também satisfaz para todo $t$ totalmente positivo. Dada uma valorização real $v$ de $F(\sqrt{t})$, sejam $v' = v/F$, $G$ e $G'$ os grupos de valores de $v$ e $v'$, respectivamente. Pelo Lema 2.32, $o(G/2G) \leq 2$ e $o(G'/2G') = 2$ se e somente se $o(G/2G) = 2$. Suponhamos que $o(G/2G) = 2$. Então, $o(G'/2G') = 2$ e, como $F$ satisfaz (2), $F_{v'}$ é euclideano. Se $G' = G$ então $[F_v : F_{v'}] = 2$. Mas, como $F_{v'}$ é euclideano $F_{v'}(\sqrt{-1})$ é a única extensão quadrática própria de $F_{v'}$. Assim, $F_v = F_{v'}(\sqrt{-1})$, o que é impossível pois $v$

é uma valorização real. Logo, $G' \subsetneq G$ e, por [E] (Corolário 17.5) temos $o(G/G') = [F(\sqrt{t}) : F] = 2$ e $F_v = F'_{v'}$, com o que $F_v$ é euclideano.

(4) $\Rightarrow$ (1) Se $F_P$ não satisfaz a L.S.F. então existem $P \in Y_{F_P}$ e $a,b \in F_P$ tais que $a,b$ e $-ab \in P$. Então $F(a,b)$ é uma extensão admissível de $F$ (pois toda extensão contida em $F_P$ é admissível) com q-ordem própria, contrariando (4).∎

A proposição 2.40 generaliza o Teorema 2.33 pois estabelece condições para a hereditariedade da L.S.F. em relação a extensões admissíveis.

Uma classe de corpos importante no estudo das formas quadráticas é a classe dos corpos henselianos, especialmente porque neles as questões de isotropia e isotropia fraca se reduzem às correspondentes questões no corpo de resíduos. Além disso, conforme mostraremos no Capítulo III, o comportamento em relação à isotropia fraca de uma forma quadrática sobre um corpo $F$ é determinado pelo seu comportamento nos fechos henselianos (de valorizações reais) e nos fechos reais (relativos às ordens arquimedianas de $F$).

No próximo parágrafo relacionaremos q-ordens de $F$ (compatíveis com $v$) com as q-ordens do fecho henseliano.

## §2. CORPOS HENSELIANOS FORMALMENTE REAIS

2.41 - DEFINIÇÃO: *Um corpo valorizado* $(F,v)$ *é um corpo 2-henseliano se para todo polinômio mônico* $f(x) \in A_v[x]$ com $\partial f = 2$ *e tal* *que exista* $a \in A_v$ *com* $f(a) \in M_v$ *e* $f'(a) \notin M_v$, *existe* $b \in A_v$ *tal que* $f(b) = 0$ e $b - a \in M_v$.

Se a definição for válida para polinômios de qualquer grau, $(F,v)$ é chamado *henseliano*.

Salvo menção em contrário sempre que falarmos em corpos henselianos nos referiremos a corpos formalmente reais.

Uma extensão $(K,w,H) \mid (F,v,G)$ de corpos valorizados é *imediata* se $H = G$ e $K_w = F_v$.

2.42 - PROPOSIÇÃO: *Seja* $(K,W,H) \mid (F,V,G)$ *uma extensão imediata de corpos valorizados. A correspondência* $Y_K^w \to Y_F^v$, $P_K \to P_K \cap F$ *é bijetora.*

DEMONSTRAÇÃO: Desde que $G = H$ podemos escolher uma q-secção de $v$ que é também uma q-secção de $w$ e como $K_w = F_v$, pela Proposição 2.24, a correspondência é bijetora. ■

Analogamente, a correspondência $X_K^w \to X_F^v$ tal que $P_K \to P_K \cap F$ é bijetora.

Listamos agora alguns resultados bem conhecidos da teoria de corpos henselianos das quais faremos uso nesse parágrafo e no Capítulo III. A demonstração desses fatos (que foge do objetivo desse trabalho) pode ser encontrada em [ E ].

2.43 - PROPOSIÇÃO: *Seja* $(F,v)$ *um corpo valorizado.*

(a) $(F,v)$ *é henseliano se e somente se a valorização* $v$ *de* $F$ *se estende de modo único a toda extensão algébrica de* $F$.

(b) *Se a característica de* $F_v$ *é zero, então* $(F,v)$ *é henseliano se e somente se não existe extensão algébrica imediata própria de* $(F,v)$.

(c) *Para todo corpo valorizado* $(F,v)$ *existe, a menos de isomorfismo de corpos valorizados sobre* $(F,v)$ *uma única extensão algébrica imediata henseliana.*

Se $(K,w)$ for a única extensão algébrica imediata henseliana de $(F,v)$ então $(K,w)$ é chamado *fecho henseliano* de $(F,v)$.

2.44 - PROPOSIÇÃO: *Se* $(F,v)$ *é um corpo 2-henseliano então*

a) $Y_F^v = Y_F$ $(X_F^v = X_F)$

b) $F$ *é pitágorico se e somente* $F_v$ *é pitagórico.*

c) $F$ *é formalmente real se e somente se* $F_v$ *é formalmente real.*

d) *Se* $v$ *é não trivial, então* $F$ *só possui* q-*ordens não arquimedianas.*

DEMONSTRAÇÃO:

a) Sejam $\leq$ uma q-ordem de $F$, $0 < a$ e $ba^{-1} \in M_v$. Então $x^2 + x + ba^{-1} \equiv x(x+1) \mod M_v$ e pelo Lema de Hensel existem $c,d \in F$ tais que $x^2 + x + ba^{-1} = (x+c)(x+d)$ com $c + d = 1$ e $ba^{-1} = cd$. Mas então, conforme [P] (1975) Teorema 8.3, $b \leq \frac{a}{4} < a$ e, portanto $\leq$ é compatível com $v$.

b) Suponhamos que $F$ seja pitagórico.

Sejam $[a]$, $[b] \in F_{v}$. Existe $c \in F$ tal que $a^2+b^2=c^2$. Logo, $[a]^2 + [b]^2 = [a^2 + b^2] = [c^2] = [c]^2$ e, portanto, $F_v$ é pitagórico.

Suponhamos que $F_v$ seja pitagórico. Sejam $a,b \in F^{\cdot}$. Se $(b/a)^2 \in A_v$ então, como $v$ é uma valorização real, $v(1+(b/a)^2) = \min\{v(1), 2v(b/a)\} = 0$, pois $v(1+(b/a)^2) > 0$ implica em $-1 = [b/a]^2$ em $F_v$. Desde que $F_v$ é pitagórico $[1 + (b/a)^2] = [1] + [b/a]^2$ existe $c \in F^{\cdot}$ tal que $[1 + b/a]^2 = [c]^2$, isto é, para $f(x) = x^2 - (1 + (b/a)^2 \in A_v[x]$, $f(c) \in M_v$. Como $f'(c) \notin M_v$ e $(F,v)$ é 2-henseliano existe $d \in F$ tal que $d^2 = 1 + (b/a)^2$ e, portanto, $a^2 + b^2 = (ad)^2 \in F^2$. Se $(b/a)^2 \notin A_v$, então $(a/b)^2 \in A_v$ e a situação é análoga à anterior.

c) Se $F$ é formalmente real, então, por 1.21, $F$ possui uma q-ordem $P$. Por (a) $P \in X_F^v$ e então, por 2.10, $F_v$ é formalmente real. Se $F_v$ é formalmente real, $v$ é uma valorização real e, por 2.11, $F$ é formalmente real.

d) Seja $P$ uma q-ordem de $F$. Por (a) $P$ é compatível com $v$ e, portanto, pela proposição 2.12, $P$ é não arquimediana. ∎

Com 2.44 (a) obtemos do Teorema 2.26, para corpos henselianos a seguinte caracterização:

2.45 - TEOREMA: *Seja* $(F,v,G)$ *um corpo 2-henseliano e* $v: F \to G$ *uma valorização real. Então,* $X_F = Y_F$ *se e somente se*

$o(G/2G) \leq 2$ e

a) *Se* $o(G/2G) = 2$ *então* $|X_{F_v}| = 1$

b) *Se* $o(G/2G) = 1$ *então* $X_{F_v} = Y_{F_v}$

A proposição 2.45 nos dá informações sobre o fecho henseliano de um corpo valorizado.

2.45 - PROPOSIÇÃO: *Sejam* $(F,v)$ *um corpo valorizado qualquer e* $(K,w)$ *o fecho henseliano de* $(F,v)$.

(i) *Se* $v$ *é uma valorização real então* $w$ *é a única valorização real de* $K$ *que estende* $v$.

(ii) $v$ *é uma valorização real se e somente se* $K$ *é formalmente real.*

DEMONSTRAÇÃO:

(i) Como por definição $(K,w)$ é uma extensão imediata de $(F,v)$, $w$ é uma valorização real de $K$ que estende $v$. Seja $w_1$ uma valorização real arbitrária de $K$ que estende $v$. Por 2.24, existe $P \in Y_K^{w_1} \subset Y_K = Y_K^w$. Então, por 2.6 $A_{w_1}$ e $A_w$ são convexos em relação a $P$. Logo, $A_{w_1} \subset A_w$ ou $A_w \subset A_{w_1}$. Como $A_w \cap F = A_{w_1} \cap F$ e $K|F$ é uma extensão algébrica , $A_w = A_{w_1}$ , isto é, $w$ e $w_1$ são equivalentes.

(ii) Pela proposição 2.44 (c) K é f.r. se e somente se $K_w = F_v$ é f.r., logo, se e somente se v é uma valorização real.■

Com as considerações feitas e os resultados enunciados, podem ainda ser obtidas as seguintes caracterizações de corpos 2-henselianos e henselianos.

2.46 - PROPOSIÇÃO: *Seja* (F,v) *um corpo valorizado e* F *formalmente real. Então* (F,v) *é* 2-*henseliano se e somente se* $1+M_v \subset F^2$.

DEMONSTRAÇÃO: Como F é formalmente real e, por 2.44 (a), $X_F^v = X_F$, v é uma valorização e car $F_v = 0$. Sejam $a \in M_v$ e $f(x) = x^2 - (1 + a) \in A_v[x]$. Temos $f \equiv x^2 - 1 \mod M_v$, $f(1) \in M_v$ e $f'(1) \notin M_v$. Assim, desde que (F,v) é 2-henseliano, existe $b \in F$ tal que $b^2 - (1 + a) = 0$, isto é, $1 + a = b^2 \in F^2$. Portanto, $1 + M_v \subset F^2$. Se $1 + M_v \subset F^2$, é imediato, pela definição, que (F,v) é 2-henseliano.■

2.47 - PROPOSIÇÃO: ([P] (1975) Teorema 8.7): *Seja* v *uma valorização real de* F. *Então* (F,v) *é henseliano se e somente se* $X_K = X_K^w$ *para toda extensão algébrica finita* (K,w) *de* (F,v).

DEMONSTRAÇÃO: Se (F,v) é henseliano, por 2.43 (a) toda extensão algébrica (K,w) de (F,v) é henseliana e, portanto, $X_K^w = X_F$.

Se $X_K = X_K^w$ para toda extensão finita (K,w) de (F,v), então toda extensão algébrica $(K,w)$ de $(F,v)$ satisfaz $X_K^w = X_K$. Seja $P \in X_F$ e $(\bar{F},\bar{P})$ o fecho real de $(F,P)$. Então $\{\bar{P}\} = \bar{X}_F = X_{\bar{F}}^{\bar{v}}$ para toda extensão $\bar{v}$ de $v$ a $\bar{F}$. Logo, toda extensão de $v$ a $\bar{F}$ é uma valorização real. Mas, por 2.30, essa extensão é única. Como $\bar{F}$ é real fechado e $\bar{v}$ é valorização real $(\bar{F},\bar{v})$ não possui extensão algébrica imediata própria e portanto, por 2.43 (b), $(\bar{F},\bar{v})$ é henseliano. Assim, por 2.43 (a), $\bar{v}$ se estende de modo único a $\bar{F}(\sqrt{-1})$. Logo, $v$ se estende de modo único a $\bar{F}(\sqrt{-1})$, que é o fecho algébrico de $F$, e, por 2.43 (a), $(F,v)$ é henseliano. ∎

## §3 - EXEMPLOS

O exemplo 2.48 mostra que dada uma q-ordem $P$ de um corpo $F$, a valorização associada ao anel $A(P,Q)$ nem sempre é compatível com $P$.

2.48 - EXEMPLO: Seja o corpo das séries formais $Q((Q))$ ( um elemento de $Q((Q))$ é da forma $\sum_{s \in Q} \mu_s Y^s$ onde $\mu_s \in Q$ e $\{s \in Q;\ \mu_s \neq 0\}$ é vazio ou bem ordenado). Consideremos o corpo $F(x)$ *onde* $F$ *é o corpo de frações do anel das séries de potências finitas de* $Q((Q))$ *e* $x$ *é uma indeterminada sobre* $F$.

Vamos considerar em $F$ duas ordens: $P_1$ definida por $\mu_1 Y^{s_1} + \dots + \mu_n Y^{s_n}$ $P_1 \leftrightarrow \mu_1 \geq 0$ e $s_1 < \dots > s_n$ em $Q$; $P_2$ definida através do $Q$-isomorfismo $\varphi: F \to \mathbb{R}$ tal que $\varphi(Y)\pi =$ e con siderando a ordem induzida de $\mathbb{R}$.

Sejam a valorização $v : \dot{F}(x) \to \mathbb{Z}$ dada por $v(x^n) = -n$, cujo corpo de resíduos é $F$ e a secção $s : \mathbb{Z} \to F(x), n \to x^{-n}$.

A aplicação $\mathcal{P} : \mathbb{Z} \to X_F$ dada por

$$\mathcal{P}(z) = \begin{cases} P_1 & \text{se } 2 \mid z \\ P_2 & \text{se } 2 \nmid z \end{cases}$$ induz em $F(x)$ pelo Teorema 2.24

uma q-ordem $P$ de $F(x)$ compatível com a valorização $v$.

Mostremos que $P$ não é compatível com a valorização $w : \dot{F}(x) \to G$ associada ao anel $A(P,Q)$.

Suponhamos que $w(Y) \leq w(1)$. Então $Y \notin M_v$ (pois $w(1)=0$) e, consequentemente, existe $a \in P^{\cdot} \cap Q$ tal que $Y - a \in P^{\cdot}$. Mas então, $[(Y - a)s(v(Y - a))^{-1}] \in \mathcal{P}(v(Y - a))$. Como $v(Y - a) = 0$ (pois $Y - a \in F$) temos que $Y - a \in P_1$ e, portanto, $-a \in P^{\cdot} \cap Q$, o que é uma contradição. Logo, $w(1) < w(Y)$ e assim $w(x) = w(1) + w(x) < w(Y) + w(x) = w(xy)$.

Mas $x - xy \notin P$. De fato: Como $v(x(1 - Y) = \{\min v(x), v(1 - Y)\} = -1$ e $\mathcal{P}(v(x - xy) = P_2$ temos que $[x(1 - Y).s(v(x - xy))^{-1}] = [x(1 - Y).x^{-1}] = 1 - Y \notin P_2$. Logo, $[x(1 - Y).sv(x - xY)^{-1}] \notin \mathcal{P}(v(x - xy))$ e isso implica que se $x - xy \notin P$.

Logo, $w$ não é compatível com $P$. ∎

Em 2.49 damos exemplo de um corpo com q-ordem própria obtida através da aplicação do Teorema 2.24 e que mostra que todo corpo de funções em duas variáveis, formalmente real, não satisfaz a L.S.F.

2.49 - EXEMPLO: *Sejam* (F,P) *um corpo ordenado e* F(x,y) *o corpo das funções racionais sobre* F *nas variáveis* x *e* y.

Consideremos em $\mathbb{Z} \times \mathbb{Z}$ a ordem lexicográfica. Seja a valorização $v : \dot{F}(x,y) \to \mathbb{Z} \times \mathbb{Z}$ dada por $v(a_n x^n y^m) = (-n,-m)$ e $v(f) = \min \{v(a_{ij}x^i y^j\}$ se $f \in F[x,y]$ e $f = \sum\limits_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} a_{ij}x^i y^j$.

Então: $A_v = \{\frac{f}{g} \in F(x,y) \ ; \ v(f) \geq v(g)\} \cup \{0\}$

$M_v = \{\frac{f}{g} \in F(x,y) \ ; \ v(f) > v(g)\} \cup \{0\}$ ,

e a aplicação $\varphi : A_v \to F$ definida por $\varphi(f/g) = a_{nm}/b_{nm}$ se $v(g) = (-n,-m)$ e $v(g) = v(f)$ e $\varphi(f/g) = 0$ se $v(g) = (-n,-m)$ e $v(g) > v(f)$ é um homomorfismo sobrejetor com núcleo $M_v$. Logo, $A_v/M_v \cong F$.

A aplicação $s : \mathbb{Z} \times \mathbb{Z} \to F(x,y)$, $(n,m) \to x^{-n}y^{-m}$ satisfaz:

a) $v(s(n,m) = v(x^{-n}y^{-m}) = (n,m)$

b) $s((n_1,m_1)+(n_2,m_2)) = s((n_1+n_2,m_1+m_2)) = x^{-(n_1+n_2)}y^{-(m_1+m_2)}$

$= s((n_1,m_1)) \, . \, s((n_2,m_2))$

c) $s((0,0)) = x^0 y^0 = 1$

d) $s(2(n,m)) = (x^{-n}y^{-m})^2 \in \dot{F}^2$

e) $s((n,m) + 2(n_1,m_1)) = x^{-n}y^{-m}(x^{-n1}y^{-m1})^2 \in s((n,m)) \, . \, \dot{F}^2$ .

Logo s é uma secção do corpo valorizado $(F(x,y), v, \mathbb{Z} \times \mathbb{Z})$.

Sejam $P^*$ a semi-ordem quadrática definida por $b - a \in P^* \leftrightarrow a - b \in P$ (observe que $1 \notin P^*$) e a aplicação $\mathcal{P}$ de $\mathbb{Z} \times \mathbb{Z}$ no conjunto das semi-ordens de $F(x,y)_v = F$ dada por:

$$\mathcal{P}((n,m)) = \begin{cases} P & \text{se } 2 \mid n \text{ ou } 2 \mid m \\ P^* & \text{se } 2 \nmid n \text{ e } 2 \nmid m. \end{cases}$$

Pelo Teorema 2.24 obtemos em $F(x,y)$ uma q-ordem $P_1(\leq)$ compatível com a valorização $v$, para a qual:

a) $x \in P_1$ pois $[x \,.\, s(v(x))^{-1}] = [x.s((-1,0))^{-1}] = [x.x^{-1}] =$
$= 1 \in P = \mathcal{P}((-1,0)) = \mathcal{P}(v(x))$.

b) $y \in P_1$ pois $[y.s(v(y))^{-1}] = [y.s((0,-1))^{-1}] = [y \,.\, y^{-1}] =$
$= 1 \in P = \mathcal{P}((0,-1) = \mathcal{P}(v(y))$.

c) $-xy \in P_1$ pois $[-xy \,.\, s(v(xy))^{-1}] = [-xy \,.\, s((-1,-1))^{-1}]$
$= [-xy \,.\, (xy)^{-1}] = -1 \in P^* = \mathcal{P}((-1,-1)) = \mathcal{P}(v(-xy))$.

Logo, $P_1$ é uma q-ordem própria de $F(x,y)$. ∎

Usando o Teorema 2.27 podemos concluir de maneira mais conceptual que se $F$ é formalmente real então $X_{F(x,y)} \neq Y_{F(x,y)}$. Basta observar que o polinômio $x - 1 \in F(y)[x]$ determina uma valorização real com grupo de valores $\mathbb{Z}$ e corpo de resíduos $F(y)$ que possui infinitas ordens.

Generalizando o exemplo 2.49 pode-se mostrar que, se $F$ é formalmente real e $K = F(x_1, x_2, \ldots)$ é uma extensão puramente transcendente com pelo menos duas variáveis então $K$ possui uma valorização real com grupo de valores $G$ tal que $o(G/2G) > 2$ e, portanto, $X_K \neq Y_K$.

Nos exemplos 2.50 e 2.51 fica claro que, se $K$ é um corpo de funções racionais em uma indeterminada, podemos ter $X_K = Y_K$ ou $X_K \neq Y_K$. No Capítulo IV mostraremos que é preciso estabelecer restrições sobre o corpo de coeficientes $F$ para que toda q-ordem de $F(x)$ seja uma ordem.

2.50 - EXEMPLO: Seja $v : \mathbb{R}(x) \to G$ uma valorização real de $\mathbb{R}(x)$. Então a restrição de $v$ a $\mathbb{R}$ ou é a valorização trivial de $\mathbb{R}$ (isto é, $v(a) = 0$ para todo $a \in \mathbb{R}$) ou uma valorização real de $\mathbb{R}$. Mas, desde que a única ordem de $\mathbb{R}$ é arquimediana, $\mathbb{R}$ não possui valorização real e, portanto, $v$ é trivial sobre $\mathbb{R}$. Logo $v$ é a valorização $p(x)$-ádica com $p(x) = x - a$ e $a \in \mathbb{R}$ (para $p(x) = ax^2 + bx + c$ irredutível sobre $\mathbb{R}$, o corpo de restos de $v_p(x)$ é $\mathbb{C}$ ) ou a valorização dada pelo grau. Nos dois casos $G \simeq \mathbb{Z}$ e $\mathbb{R}(x)_v \simeq \mathbb{R}$. Logo, por 2.27, $\mathbb{R}(x)$ satisfaz $X_{\mathbb{R}(x)} = Y_{\mathbb{R}(x)}$. ■

2.51 - EXEMPLO: Seja o corpo $Q(x)$. O polinômio $x^2 - 2$ determina uma valorização real de $Q(x)$ trivial sobre $Q$ com grupo de valores $\mathbb{Z}$ e corpo de restos isomorfo a $\frac{Q[x]}{x^2 - 2} \simeq Q(\sqrt{2})$ que admite duas ordens. Logo, $Q(x)$ não satisfaz $X_{Q(x)} = Y_{Q(x)}$. ■

2.52 - EXEMPLO: Seja o corpo das séries formais $F((x))$.

A aplicação $v : F((x)) \to F$ definida por $v(\sum_{i=m}^{\infty} a_i x_i) = m$ se $a_m \neq 0$ é uma valorização de $F((x))$ com anel de valorização

$A_v = F[[x]]$ ideal maximal $M_v = (x)$ e, portanto, corpo de restos $F((x))_v = A_v/M_v \cong F$. Conforme [E] (5.8), $(F((x)),v,\mathbb{Z})$ é o completamento do corpo valorizado $(F(x),v_x,\mathbb{Z})$, onde $v_x$ é a valorização x-ádica. E, por [E] (16.7), $(F((x)),v)$ satisfaz o Lema de Hensel. Logo, se $F$ for formalmente real, $v$ é a única valorização real de $F((x))$. E, portanto, pelo Teorema 2.27, $X_{F((x))} = Y_{F((x))}$ se e somente se $|X_F| = 1$. Assim, $\mathbb{R}((x))$ e $Q((x))$ satisfazem a L.S.F. e $Q(\sqrt{2})((x))$ não satisfaz. Em $\mathbb{R}((x))$ a L.S.F. é hereditária (pelo Teorema 2.33). ∎

2.53 - EXEMPLO: Seja $k$ um corpo euclideano mas não hereditariamente euclideano. O corpo $k((x))$ satisfaz a L.S.F. mas não satisfaz a L.S.F. hereditariamente. Como $k((x)) = k((x))_p$ (= fecho pitagórico de $k((x))$), $k((x))$ satisfaz a hereditariedade da L.S.F. em relação a extensões admissíveis. ∎

2.54 - EXEMPLO: Sejam $F$ um corpo formalmente real e $K=F((x))((y))$. Temos $X_K \neq Y_K$ pois $|X_{F((x))}| > 1$, visto que para toda ordem $\leq$ de $F$ existem duas ordens de $K$ que a estendem uma na qual $x$ é positivo e outra na qual $x$ é negativo ([L] Capítulo VIII Proposição 5.9). ∎

2.55 - EXEMPLO: Sejam $R_1$ e $R_2$ dois fechos reais de $Q$ que induzem ordens diferentes em $Q(\sqrt{2})$ e $R = R_1 \cap R_2$. O corpo $R$ é pitagórico e possui duas ordens. Por 2.44 (b), o corpo $R((x))$ é pitagórico. Pelo exemplo 2.52 $R((x))$ não satisfaz a L.S.F. ∎

2.56 - EXEMPLO: Sejam $R$ o fecho algébrico de $Q$ em $\mathbb{R}$, $x_1,\ldots,x_n \in \mathbb{R}$ elementos algebricamente independentes sobre $\mathbb{R}$ e $x \in \mathbb{R}$ um elemento transcendente sobre $R$ e positivo.

a) O corpo $F = R(x_1,\ldots,x_n)$ não satisfaz a L.S.F. pois, desde que $x_1$ e $x_2$ são algebricamente independentes sobre $R$, a forma $<1,x_1,x_2,-x_1x_2>$ que é totalmente indefinida, não é fracamente isotrópica sobre $R$.

b) O corpo $F(x)$ também não satisfaz a L.S.F.. O polinômio $x - 1$ determina uma valorização real de $F(x)$ cujo grupo de valores é $\mathbb{Z}$ e cujo corpo de restos é $F$, que possui mais de uma ordem (pois não satisfaz a L.S.F.).

c) O corpo $K = F(x)(\sqrt[2^m]{x})$ com $m \in \mathbb{N}^{\cdot}$ não satisfaz a L.S.F.. $K$ possui uma valorização real cujo corpo de resíduos é $F(\sqrt[2^m]{x})$, que possui mais de uma ordem, pois $|X_{F(\sqrt[2^m]{m})}| = 1$ implica que $|X_F| = 1$. ∎

# CAPÍTULO III

## PRINCÍPIOS DE NATUREZA LOCAL-GLOBAL

## REFERENTES A ISOTROPIA FRACA

No Capítulo I mostramos que a isotropia fraca de uma forma quadrática $\rho$ sobre um corpo ordenado $F$ pode ser analisada pela isotropia de $\rho$ nos fechos reais de $F$ se e somente se $X_F = Y_F$. A caracterização dada no Capítulo II mostra o quanto é restrita essa classe de corpos.

Nesse Capítulo apresentamos resultados que dão condições necessárias e suficientes à isotropia fraca de uma forma quadrática sobre um corpo ordenado qualquer.

O Princípio Local Global de Hasse-Minkowski reduz a questão da isotropia num corpo global $F$ à respectiva questão nos completamentos relativos às topologias induzidas pelas valorizações de $F$. Os Teoremas 3.2 e 3.8 desse Capítulo mostram que a questão da isotropia fraca em $F$ pode ser reduzida à respectiva questão nos completamentos relativos às ordens de $F$ ou à respectiva questão nos fechos reais de $F$ relativos às ordens arquimedianas e henselizações relativas as valorizações reais de $F$.

## §1 - RELATIVO A COMPLETAMENTOS

Se $F$ é um corpo formalmente real e $P$ é uma q-ordem de $F$ então $P$ define em $F$ a topologia intervalo aberto $\tau_P$, compatível com a estrutura de corpo de $F$.

Uma base de vizinhanças abertas da origem em $\tau_P$ é dada pela família de intervalos $(-\varepsilon,\varepsilon)$ com $\varepsilon \in P^{\cdot}$ e $1-\varepsilon \in P^{\cdot}$.

Se $(F,P)$ é um corpo ordenado o completamento de $F$ relativo a $\tau_P$ é uma extensão ordenada de $(F,P)$. Denotaremos esse completamento por $(\hat{F},\hat{P})$. Se a ordem $P$ é arquimediana $(\hat{F},\hat{P})$ é isomorfo a $\mathbb{R}$. A proposição 3.1 mostra que se $P$ não é arquimediana então $(\hat{F},\hat{P})$ coincide com os completamentos $(\hat{F},\hat{v})$ de $F$ relativos as topologias $\tau_v$ definidas em $F$ pelas valorizações reais $v$ de $F$ compatíveis com $P$.

Lembramos que em $\tau_v$ um sistema fundamental de vizinhanças da origem é dado pelos conjuntos $v(0,g)=\{y \in F; v(y) > g\}$ para $g \in G$ e $g > 0$.

3.1 - PROPOSIÇÃO: *Se* $(F,P)$ *é um corpo* q-*ordenado e* $v: \dot{F} \to G$ *é uma valorização de* $F$ *tal que* $A_v$ *é convexo relativamente a* $P$ *então* $\tau_v = \tau_P$.

DEMONSTRAÇÃO: (Nota: O símbolo $\leq$ será usado para a ordem de $G$ e também com o significado de $a \leq b$ se e somente se $a-b \in P$, quando $a, b \in F$).

Seja $v(0,g)$ um aberto básico do sistema fundamental de vizinhanças da origem em $\tau_v$ e $\delta \in F$ tal que $v(\delta)=g$.

Tomando $\varepsilon = \delta^2$ temos, para todo $a \in F$ tal que $a \in (-\varepsilon, \varepsilon)$, $a \in v(0,g)$. Basta ver que : $|a| < \varepsilon = \delta^2 \Rightarrow |a\delta^{-2}| < 1 \Rightarrow a\delta^{-2} \in A_v$ (pois $A_v$ é convexo relativamente a $P$) $\Rightarrow v(a\delta^{-2}) \geq 0 \Rightarrow v(a) \geq$ $\geq v(\delta^2) = 2v(\delta) = 2g > g$.

Por outro lado, seja $(-\varepsilon,\varepsilon)$ um aberto básico qualquer do sistema fundamental de vizinhanças da origem na topologia $\tau_P$ e $g = v(\varepsilon^2)$. Para todo $a \in F$ tal que $a \in v(0,g)$ vale: $\pm a\varepsilon^{-2} \in$ $\in M_v$, pois, $a \in v(0,g) \Rightarrow v(a) > g \Rightarrow v(a) - g = v(a) + v(\varepsilon^{-2}) =$ $= v(a\varepsilon^{-2}) > 0$. Se $1 < |a\varepsilon^{-2}|$ então $|a^{-1}\varepsilon^2| < 1$ e, pela convexidade de $A_v$ relativamente a $P$, $\pm a^{-1}\varepsilon^2 \in A_v$, contrariando $\pm a\varepsilon^{-2} \in M_v$. Logo $|a\varepsilon^{-2}| < 1$ e $|a| < \varepsilon^2 < \varepsilon$, isto é, $a \in (-\varepsilon,\varepsilon)$. ∎

Observamos que se $(F,P)$ é não arquimediano então, pelo Teorema 2.14, $F$ possui um anel de valorização real, convexo relativamente a $P$. E mais, como o anel $A(P,Q)$ é convexo relativamente a $P$, pela Proposição 3.1, todas as topologias definidas em $F$ por anéis de valorização convexos relativamente a $P$ coincidem com a topologia de Hahn como é usualmente denominada a topologia das classes arquimedianas associada ao anel $A(Q,P)$.

Reciprocamente, se $v : \dot{F} \to G$ é uma valorização real de $F$ então existe uma ordem não arquimediana $P$ de $F$ tal que $\tau_v = \tau_P$.

3.2 - TEOREMA: *Seja $F$ um corpo. Uma forma quadrática $\rho$ sobre $F$ é fracamente isotrópica em $F$ se e somente se $\rho$ é fracamente isotrópica em $(\hat{F},\hat{P})$ para todo $P \in X_F$.*

Ou equivalentemente:

3.2' - TEOREMA: Seja $F$ um corpo. *Uma forma quadrática* $\rho$ *sobre* $F$ *é fracamente isotrópica em* $F$ *se e somente se* $\rho$ *é fracamente isotrópica em* $(\hat{F},\hat{P})$ *para toda ordem arquimediana e em* $(\hat{F},\hat{v})$ *para toda valorização real de* $F$.

Na demonstração do Teorema é usado o seguinte lema:

3.3 - LEMA: *Dada uma* q-*ordem* $P$ *de um corpo* $F$ *existe uma ordem* $P'$ *de* $F$ *tal que as topologias* $\tau_P$ *e* $\tau_{P'}$ *coincidem.*

PROVA: Seja $P$ uma q-ordem de $F$. Podemos assumir $P$ não arquimediana pois, por 1.16, toda q-ordem arquimediana é uma ordem. Então, por 2.14, existe uma valorização real $w$ de $F$ compatível com $P$. Por 2.6, $A_w$ é convexo relativamente a $P$ e, portanto, pela Proposição 3.1, $\tau_w = \tau_P$. Como $w$ é uma valorização real, por 2.24 e 2.25, existe uma ordem $P'$ de $F$ compatível com $w$. Logo $A_w$ é convexo relativamente a $P'$ e $\tau_w = \tau_{P'}$.■

DEMONSTRAÇÃO DO TEOREMA 3.2: $(\Rightarrow)$ Se $\rho$ é fracamente isotrópica em $F$ é imediato que $\rho$ é fracamente isotrópica em $(\hat{F},\hat{P})$ para todo $P \in X_F$.

$(\Leftarrow)$ Suponhamos que $\rho = \langle a_1,\ldots,a_n\rangle$ seja uma forma quadrática fracamente isotrópica em $(\hat{F},\hat{P})$ para todo $P \in X_F$ e que $\rho$ não é fracamente isotrópica em $F$. Pela Proposição 1.30, existe uma q-ordem $P_q$ de $F$ tal que $a_i \in P_q$ para todo $1 \leq i \leq n$ ou $-a_i \in P_q$ para todo $1 \leq i \leq n$. Pelo Lema 3.3 existe $P \in X_F$ tal que $\tau_P = \tau_{P_q}$. Seja $(\hat{F},\hat{P})$ o completamento de $F$ relativo à $\tau_P$. O conjunto $\hat{P}_q = \{a \in \hat{F};\ \forall\ U_a \subset \tau_{\hat{P}},\ U_a \cap \cap\ P_q \neq \emptyset\}$ é um q-cone positivo de $\hat{F}$ que estende $P_q$. Basta observar que $P_q \subset \hat{P}_q$ e que $\hat{P}_q$ satisfaz as propriedades $\hat{P}_q + \hat{P}_q \subset P_q$, $P \cup -\hat{P}_q = \hat{F}$, $a^2\hat{P}_q \subset \hat{P}_q$ para todo $a \in \hat{F}$ e $\hat{P}_q \cap -\hat{P}_q = \{0\}$. Assim, $\rho$ é definida relativamente a uma q-ordem. Por 1.30, $\rho$ é então, fortemente anisotrópica em $(\hat{F},\hat{P})$, e isso é uma contradição. ∎

Porém, de modo geral, dado um corpo $F$ nada se pode concluir a respeito da isotropia de uma forma quadrática $\rho$ sobre $F$ sabendo que $\rho$ é isotrópica nos completamentos $(\hat{F},\hat{P})$ de $F$. A forma $\rho = <1,-3>$ sobre $\mathbb{Q}$ é claramente isotrópica em $\mathbb{R}$, que é o completamento de $\mathbb{Q}$ relativo à sua única ordem, mas não é isotrópica em $\mathbb{Q}$.

O Teorema 3.2 lembra, no entanto, dois resultados clássicos referentes à questão da isotropia.

O primeiro, é o Corolário do Princípio Local-Global de Hasse-Minkowski, já citado no Capítulo II:

*Se $F$ é um corpo de números algébricos e $\rho$ é uma forma quadrática sobre $F$ de dimensão maior ou igual a 5 então $\rho$ é isotrópica em $F$ se e somente se $\rho$ é isotrópica em $(\hat{F},\hat{P})$ para todo $P \in X_F$.*

Observamos que nesse caso $F$ só possui ordens arquimedianas e portanto não existe valorização real de $F$.

O segundo é um teorema de Witt e é de um corpo em que todas as ordens são não arquimedianas:

*Se* $F$ *é uma extensão algébrica do corpo de funções racionais* $\mathbb{R}(x)$ *e* $\rho$ *é uma forma quadrática sobre* $F$ *tal que* $\dim \rho \geq 3$ *então* $\rho$ *é isotrópica em* $F$ *se e somente se* $\rho$ *é isotrópica em* $(\hat{F},\hat{v})$, *para toda valorização real de* $F$.

No Capítulo IV ficará claro que esse resultado é mais geral. Ele continua válido se $F$ for uma extensão finita de $F_0(x)$ com $F_0$ hereditariamente euclideano.

## §2 - RELATIVO A HENSELIZAÇÕES

Nosso objetivo, agora, é relacionar a isotropia fraca num corpo formalmente real $F$ com a isotropia fraca nos fechos henselianos de $F$ relativos às valorizações reais de $F$.

Sejam $v : \dot{F} \to G$ uma valorização de $F$, $s : G \to \dot{F}$ uma q-secção de $v$ e $\rho = \langle a_1,\ldots,a_n\rangle$ uma forma quadrática sobre $F$. Desde que estamos interessados apenas na questão da isotropia e isotropia fraca podemos escrever $\rho$ como $\rho = \rho^{(1)} \oplus\ldots\oplus \rho^{(m)}$ onde $\rho^{(1)} = \langle a_{i1},\ldots,a_{in_i}\rangle$ e os $a_{ij}$ são todos os $a_i$ de $\rho$ tais que os $v(a_i)$ pertencem a uma mesma classe residual de $G/2G$. Desde que para todo $a \in \dot{F}$ $a/s\,v(a) \in U_v$ $\rho$ define em $F_v$ as formas $\rho_v^{(i)} = \langle [a_{i1}/s(v(a_{i1}))],\ldots,[a_in_i/sv(a_{in_i})]\rangle$ que chamaremos de *classes residuais de* $\rho$ *em* $F_v$. Temos então $\rho_v = \rho_v^{(1)} \oplus\ldots\oplus \rho_v^{(m)}$.

3.4 - TEOREMA: *Sejam* $F$ *um corpo,* $v : \dot{F} \to G$ *uma valorização* *de* F *tal que car* $F_v \neq 2$, $\rho = \rho^{(1)} \perp \ldots \perp \rho^{(m)}$ *uma forma quadrática sobre* F *e* $\rho_v^{(1)}, \ldots, \rho_v^{(m)}$ *as classes residuais de* $\rho$ *em* $F_v$.

i) *Se* $\rho$ *é isotrópica em* F *então existe uma forma* $\rho_v^{(i)}$ *sobre* $F_v$ *que é isotropica em* $F_v$.

ii) *Se alguma forma* $\rho_v^{(i)}$ *é isotrópica em* $F_v$ *e* (F,v) *é um corpo henseliano então* $\rho$ *é isotrópica em* F.

DEMONSTRAÇÃO:

i) Seja $\rho = \langle a_1, \ldots, a_n \rangle$. Como $\rho$ é isotrópica em F, existem $b_i \in F$ $(i = 1, \ldots, n)$ não todos nulos tais que $\sum_{i=1}^{n} a_i b_i^2 = 0$. Sejam $j (1 \leq j \leq n)$ tal que $v(a_j b_j^2) = \min_{1 \leq i \leq n} \{v(a_i b_i^2)\}$ e $\rho^{(j)} = \langle a_j, a_{j2}, \ldots, a_{jn_j} \rangle$. Vamos mostrar que a classe residual $\rho_v^{(j)}$ é isotrópica em $F_v$.

Sem perda de generalidade podemos assumir $j = 1$ e $\rho^{(j)} = \langle a_1, \ldots, a_r \rangle$ com $r < n$. Como $\sum_{i=1}^{n} a_i b_i^2 = 0$, $\sum_{i=1}^{n} a_i b_i^2 / s(v(a_1) b_1^2 = 0$ e portanto $\sum_{i=1}^{r} a_i b_i^2 / s(v(a_1)) b_1^2 = - \sum_{i=r+1}^{n} a_i b_i^2 / s(v(a_1)) b_1^2$. Assim

$v(\sum_{i=1}^{r} a_i b_i^2 / s(v(a_1)) b_1^2) = v(\sum_{i=r+1}^{n} a_i b_i^2 / s(v(a_1)) b_1^2)$ e $v(a_1 b_1^2 /$

$/ s(v(a_1)) b_1^2 + \ldots + a_r b_r^2 / s(v(a_1)) b_r^2) \geq -v(a_1) - v(b_1^2) + \min_{r+1 \leq i \leq n} \{v(a_i b_1^2)\} >$

$> - v(a_1) - v(b_1^2) + v(a_1 b_1^2) = 0$. Como $v(a_1) = v(a_k) \bmod 2G$ para $1 \leq k \leq r$ implica em $s(v(a_1)) = s(v(a_k)) . c_k^2$ para $1 \leq k \leq r$

e $c_k \in \dot{F}$, temos: $v(a_1b_1^2/s(v(a_1))b_1^2+\ldots+a_rb_r^2c_r^2/s(v(a_r))b_1^2) > 0$

e $v(a_1/s(v(a_1)+a_2/s(v(a_2)).(b_2c_2/b_1)^2+\ldots+a_r/s(c(a_r).(b_rc_r/b_1)^2) > 0$

isto é, $[a_1/s(v(a_1))]+[a_2/s(v(a_2))][b_2c_2/b_1]^2+\ldots+[a_r/s(v(a_r))].[b_ra_r/b_1]^2$ $= 0$ e portanto $\rho_v^{(j)}$ é isotropia em $F_v$.

ii) Seja $\rho^{(\ell)} = \langle c_1,\ldots,c_r\rangle$ uma subforma de $\rho$ tal que a classe residual $\rho_v^{(\ell)}$ é isotrópica em $F_v$. Existem $b_1,\ldots,b_r \in A_v$ não todos pertencentes a $M_v$ tais que $\Sigma c_ib_i^2/s(v(c_i)) \in M_v$.

Sem perda de generalidade, podemos supor que $b_1 \notin M_v$. Então, para $f(x) = c_1/s(v(c_1)x^2 + \sum_{i=2}^{r} c_ib_i^2/s(v(c_i) \in A_v[x]$

$f(b_1) \in M_v$ e $f'(b_1) \notin M_v$. Logo, pelo Lema de Hensel existem $d_i \in F$ não todos nulos tais que $\sum_{i=1}^{r} c_id_i^2/s(v(c_i))=0$. Desde que $s(v(c_1) \equiv s(v(c_j)$ mod $\dot{F}^2$ para todo $1 \leq j \leq r$ pois $v(c_1) \equiv v(c_j)$ mod $2G$, temos que $\rho^{(\ell)}$ é isotrópica em $F$ e portanto $\rho$ é isotrópica em $F$. ∎

3.5 - OBSERVAÇÃO: Se em ii) não assumirmos $(F,v)$ henseliano de $v(\sum_{i=1}^{r} c_ib_i^2/s(v(c_i)) > \min\{v(c_ib_i^2/s(v(c_i))\} = 0$ obtemos apenas que existem $d_i \in F$ não todos nulos tais que $\min_{1\leq i\leq r}\{v(a_id_i^2)\} < v(\sum_{i=1}^{r} a_id_i^2)$.

O Teorema 3.4 mostra, em particular, que para corpos henselianos (F,v) a questão da isotropia se reduz à correspondente questão no corpo de resíduos $F_v$. O que leva a pensar que a questão da isotropia num corpo arbitrário F pode ser reduzida às henselizações de (F,v) onde v percorre um conjunto conveniente de valorizações de F. Um exemplo bem conhecido desse processo é o já citado Princípio Local Global de Hasse-Minkowski onde são considerados os completamentos relativos às valorizações. Mas esses completamentos são henselianos.

No caso da isotropia fraca apenas os fechos henselianos relativos às valorizações reais são relevantes e em conexão com as valorizações reais as q-ordens do corpo, como mostraremos em 3.6 e 3.7.

Para a demonstração de 3.6 necessitamos um lema técnico.

3.6 - LEMA: *Sejam* G *um grupo aditivo ordenado,* $x \in G$, $y \in G$ *com* $x < y$. *Se existem* $m \in \mathbb{N}$ *e* $g_1 \in G$ *tais que* $0 < x + 2g_1 < m(y - x)$ *então existe* $g \in G$ *tal que* $x \leq 2g \leq y$.

PROVA: Seja m o menor número natural com a propriedade citada na hipótese. Então $(m - 1)(x - y) \leq x + 2g_1 < m(y - x)$.

Se $m = 2n + 1$, com $n \in \mathbb{N}$ temos: $2n(x - y) \leq x + 2g_1 < (2n + 1)(y - x)$ é portanto $0 \leq x + 2g_1 - 2n(x - y) < y - x$.

Se $m = 2n$, com $n \in \mathbb{N}$ temos: $(2n - 1)(y - x) - (2n-2)(y-x) \leq x + 2g_1 - (2n - 2)(y - x) < 2n(y-x) - (2n - 2)(y - x)$ e portanto $y - x \leq x + 2g_1 - 2(n - 1)(y - x) < 2(y - x)$. Logo basta analisar as situações:

a) $0 \leq x + 2g_1 < y - x$

Nesse caso $g = x + g_1$ satisfaz $x \leq 2g \leq y$, pois $0 \leq x + 2g_1 \leq y - x$ implica que $x \leq 2(x + g_1) < y$.

b) $y - x \leq x + 2g_1 < 2(y - x)$.

Nesse caso $g = 2(y - x - g_1)$ satisfaz $x < 2g \leq y$, pois, $y - x \leq x + 2g_1 < 2(y - x)$ implica que $-y \leq 2x + 2g_1 - 2y < -x$ e portanto $x < 2(y - x - g_1) < y$.∎

3.7 - TEOREMA: Seja $F$ um corpo formalmente real e $\rho$ uma forma quadrática sobre $F$.

*$\rho$ é fracamente isotrópica em $F$ se e somente se:*

*i) $\rho$ é isotrópica nos fechos reais de $F$ e*

*ii) $\rho$ é fracamente isotrópica nos fechos henselianos de $F$ relativos às valorizações com grupo de valores não 2-divisível.*

DEMONSTRAÇÃO: Seja $\rho = \langle a_1, \ldots, a_n \rangle$. Suponhamos que $\rho$ não é fracamente isotrópica. Então $\rho$ é definida relativamente a alguma q-ordem $P$ de $F$ (ver 1.30). Por i) $P$ é uma q-ordem própria de $F$ e portanto é não-arquimediana. Assumamos $a_i \in \dot{P}$ para todo $1 \leq i \leq n$ e seja $v : \dot{F} \to G$ a valorização real de $F$ associada ao anel $A(P,Q)$.

Assumamos primeiro que $v(a_i) \in 2G$ para todo $1 \leq i \leq n$. Como $v(a_i) = 2g$ implica que existe $c \in F$ tal que $v(a_i) = v(c^2)$ e portanto $v(a_i c^{-2}) = 0$, podemos assumir que $a_i \in U_v$ para todo $1 \leq i \leq n$. Como $A_v$ é convexo relativamente a $P$, $A_v \cap P/M_v$

é um q-ordem de $F_v$ que por ser arquimediana é uma ordem. Por 2.24 e 2.25 existe uma ordem $P'$ de $F$ tal que $A_v \cap P'/M_v = P \cap A_v/M_v$. Logo $a_i \in P'$, para todo $1 \leq i \leq n$ e, portanto, $\rho$ e definida em relação a $P'$ contrariando a hipótese de $\rho$ ser isotrópica em todos os fechos reais de $F$.

Suponhamos agora que para algum $a_i, v(a_i) \notin 2G$. Para todo $1 \leq i \leq n$ definimos:

$G_i = \{g \in G$ para os quais não existem $n \in \mathbb{N}$ e $h \in G$ tais que $0 \leq g_i + 2h < n|g|$ , onde $g_i = v(a_i)$.

Cada $G_i$ é um subgrupo convexo de $G$ pois: se $g \in G$, $g' \in G$, $0 < g' < g$ e $g \in G_i$ então, para qualquer $h \in G$ tal que $0 \leq g_i + 2h$, $g_i + 2h > n|g|$ para todo $n \in \mathbb{N}$ e portanto, para qualquer $h \in G$ tal que $0 \leq g_i + 2h$, $g_i + 2h > n|g'|$ ,isto é, $g' \in G_i$.

Desde que $G$ é um grupo ordenado a família dos subgrupos convexos de $G$ é totalmente ordenada em relação à inclusão e portanto $G' = \bigcup_{i=1}^{n} G_i$ é um subgrupo convexo de $G$. Logo, por 2.4, o grupo quociente $G^* = G/G'$ pode ser ordenado pela relação:

$$g_1 + G' < g_2 + G' \leftrightarrow g_1 < g_2 \text{ e } g_2 - g_1 \notin G'.$$

Como a projeção canônica $p : G \to G/G'$ é um epimorfismo de grupos ordenados a aplicação $w : F \to G/G'$ com $w(a)=v(a)+ G'$ é uma valorização de $F$.

Mostremos que por construção $G^* = G/G'$ não é 2-divisível: Temos que $G' = G_i$ para algum $1 \leq i \leq n$. Se $g_i \in 2G$

então $g_i = 2h$ para algum $h \in G$ e $0 < g_i - 2h < |g|$ para todo $g \in G^{\cdot}$. Logo $g_i \in 2G$ implica que $G_i = \{0\}$ e portanto $G' = G_i$ para algum $i$ tal que $g_i \notin 2G$. Suponhamos que $g_i + G' \in 2G^*$, isto é, $g_i + G' = 2h + G'$ com $h \in G$. Mas então $g_1 - 2h \in G'$, o que é uma contradição pois:

a) $g_i - 2h > 0 \Rightarrow 0 \leq g_i - 2h < 2|g_i - 2h| \Rightarrow g_i - 2h \notin G_i = G'$

b) $g_i - 2h < 0 \Rightarrow 0 \leq g_i + 2(-g_i + h) < 2(-g_i + 2h) = 2|g_i - 2h| \Rightarrow$

$$\Rightarrow g_i - 2h \notin G_i = G.$$

Logo $g_i \notin 2G^*$ e $G^*$ não é 2-divisível.

Como $v$ é uma valorização real, existe uma ordem $P'$ de $F$ compatível com $v$. Mas então $A_w$ é compatível com $P'$. Logo $w$ uma valorização real com grupo de valores não 2-divisível. Assim, para algum $m \in \mathbb{N}$, $m\rho$ é isotropica no fecho henseliano de $(F,w)$, com o que, pelo Teorema 3.4(i) alguma classe residual de $m\rho$ em $F_w$ é isotrópica em $F_w$. Assim, por 3.5, existem $\alpha_i \in F$ não todos nulos tais que $\min_{1 \leq j \leq mn} \{w(c_j\alpha_j^2)\} < w(\sum_{j=1}^{mn} w(c_j\alpha_j^2)$ onde $c_{ij} \in \{a_1, \ldots, a_n\}$ para todo $j, 1 \leq j \leq mn$. Seja $w(c\,\alpha^2) = \min \{w(c_j\alpha_j^2)\}$. Então, $w(c) < w(\sum_{j=1}^{mn} c_j (\frac{\alpha_j}{\alpha})^2$. Logo existe $i \in \{1, \ldots, n\}$ e $p \in P$ tal que $w(a_i) < w(a_i + p)$. Mas então $v(a_i) < v(a_i + p)$ e existem $m \in \mathbb{N}$ e $g_1 \in G$ tais que $0 \leq (a_i) + 2g_1 < m(v(a_i + p) - v(a_i))$. Pelo Lema 3.6 existe, então, $g \in G$ tal que $v(a_i) \leq 2g \leq v(a_i + p)$. Assim, pela Proposição 2.7, temos

$a_i - (a_i + p) = -p \in P$, o que é uma contradição. E, portanto $\rho$ é fracamente isotrópica.

Desde que a implicação no outro sentido é imediata, o teorema fica demonstrado. ■

De 3.7 obtemos em 3.8 um Princípio Local Global que vale não só para formas quadráticas mas para toda forma de grau par. Nosso interesse é pelo caso das formas quadráticas. O caso geral pode ser encontrado em [ B ] (1980).

3.8 - TEOREMA: *Seja* F *um corpo formalmente real e* $\rho$ *uma forma quadrática sobre* F .

$\rho$ é fracamente isotrópica em F se e somente se

i) $\rho$ é fracamente isotrópica nos fechos henselianos da valorizações reais de F e

ii) $\rho$ é isotrópica nos fechos reais de F relativos às ordens arquimedianas de F.

DEMONSTRAÇÃO: Seja $\rho = \langle a_1,\ldots,a_n\rangle$. Pelo Teorema 3.7 é suficiente mostrar que $\rho$ é indefinida relativamente às ordens não arquimedianas de F. Seja P uma ordem não arquimediana de F. Por 2.14, $P \in X_F^V$ para alguma valorização real de F. Seja $(F_1,v_1)$ o fecho henseliano de $(F,v)$. Então, por 2.42, existe $P_1 \in X_{F_1}$ tal que $P_1 \cap F = P$. Desde que $\rho$ é fracamente isotrópica em $(F_1,v_1)$, $\rho$ é indefinida relativamente a ordem P, isto é, $\rho$ é isotrópica no fecho real de $(F,P)$. ■

Observamos que para os corpos nos quais toda forma quadrática fracamente isotrópica é isotrópica, como, por exemplo, os corpos pitagóricos, esse resultado vale também para a questão da isotropia. Mas, de modo geral não existe um teorema de natureza local global semelhante a esse para isotropia.

# CAPÍTULO IV

## ISOTROPIA FRACA EM CORPOS DE FUNÇÕES ALGÉBRICAS

Pelo Teorema 2.27 uma condição necessária para que num corpo $F$ seja válida a L.S.F. é que o grupo de valores $G$ de qualquer valorização real de $F$ satisfaça $o(G/2G) \leq 2$. No Corolário 2.34 mostramos que se as valorizações reais de um corpo $F$ possuem grupo de valores 2-divisível então $F$ e suas extensões algébricas satisfazem a Lei de Sylvester Fraca. Neste Capítulo analisaremos essa Lei na classe dos corpos de funções racionais em uma variável. Tais corpos admitem grupo de valores $G$ com $o(G/2G)=2$.

No §1 mostraremos que num corpo de funções racionais $F(x)$ a existência ou não existência de q-ordens próprias, ou seja, a validade da L.S.F., é determinada pelo corpo de coeficientes $F$. Mostraremos, também, que para extensões algébricas finitas de $F(x)$ vale o "going down" e a hereditariedade da L.S.F.

No §2 daremos dois princípios de natureza local-global para $F(x)$ e suas extensões finitas. O primeiro é, para corpos de funções algébricas, o Princípio de Hasse-Minkowski referente a isotropia fraca. Nesse princípio são considerados os completamentos relativos a um conjunto específico de ordens de $F$. O segundo é o Princípio de Hasse-Minkowski para corpos de funções algébricas e é obtido analisando a Lei de Sylvester: "Toda forma quadrática localmente isotrópica é isotrópica".

## §1 - A LEI DE SYLVESTER FRACA EM $F(x)$

Na análise da L.S.F. em corpos de funções algébricas tem importância fundamental os corpos hereditariamente euclideanos, já citados no Capítulo II.

Na literatura podem ser encontradas caracterizações desses corpos. Condições equivalentes da definição e uma caracterização, através da teoria de valorizações, que permite obter exemplos de corpos h.e. que não são reais fechados, são encontradas num trabalho de Prestel e Ziegler ([PZ]).

Os corpos euclideanos também foram estudados e caracterizados por Becker ([B](1978)). Ele estabelece para fechos euclideanos resultados correspondentes à teoria dos fechos reais e mostra que o Princípio Local Global de Pfister é válido para fechos euclideanos.

Mencionaremos, sem demonstração, alguns dos resultados que usaremos no desenvolver deste capítulo.

4.1 - TEOREMA([PZ] Satz 1.2): *Sejam* $F$ *um corpo formalmente real e* $\tilde{F}$ *o seu fecho algébrico. As seguintes afirmações são equivalentes:*

(1) $F$ *é hereditariamente euclideano.*

(2) $[\tilde{F} : F] = 2.n$ *onde* $n$ *é um número super natural ímpar.*

(3) *Toda extensão algébrica formalmente real de* $F$ *tem grau ímpar.*

(4) *Todo polinômio irredutível de* $F[x]$ *possui no máximo uma raiz num fecho real de* $F$.

(5) *Toda extensão algébrica de* $F(\sqrt{-1})$ *é quadraticamente fechada.*

(6) *Cada dois fechos reais de* $F$ *induzem sobre sua intersecção a mesma ordem* (isto é, são isomorfos sobre sua intersecção).

Decorre desse teorema que, se $F$ é h.e. então, $\sqrt{-1}$ pertence a toda extensão não formalmente real de $F$. Não vale, porém, a recíproca. O corpo das séries formais $\mathbb{R}((x))$ é um contra-exemplo. De fato: Seja $K$ uma extensão finita não formalmente real de $\mathbb{R}((x))$. A valorização de $\mathbb{R}((x))$ dada por $v(\sum_{i=m}^{\infty} a_i x^i) = m$ se $a_m \neq 0$ se estende a uma valorização $v_K$ de $K$. Como $K$ não é formalmente real, $K_{v_K}$ não é formalmente real e portanto isomorfo a $\mathbb{C}$, pois é uma extensão algébrica de $\mathbb{R}$. Assim, para $z^2 + 1 \in A_v[x]$ existe $\alpha \in A_v$ tal que $\alpha^2 + 1 \in M_v$. Desde que $(\mathbb{R}((x)), v)$ é henseliano, $(K, v_K)$ também é henseliano. Logo, existe $\beta \in A_v$ tal que $\beta^2 + 1 = 0$, isto é, $\sqrt{-1} \in K$. Por outro lado, $\mathbb{R}((x))$ possui duas ordens ( [L] Capítulo VII Proposição 5.9) e, portanto, não é euclideano.

O seguinte teorema dá uma caracterização dos corpos h.e. através de valorizações:

4.2 - TEOREMA([PZ] Satz 2.1): *Sejam* $F$ *um corpo e* $v : F \to G$ *uma valorização real. O corpo* $F$ *é hereditariamente euclideano* *se e somente se:*

(1) $(F,v)$ *é 2-henseliano.*

(2) *O grupo de valores de* $v$ *é 2-divisível.*

(3) *O corpo de restos de* $v$ *é hereditariamente euclideano.*

É interessante comparar 4.2. com o seguinte teorema de Prestel sobre corpos reais fechados.

4.3 - TEOREMA ([P] (1975) Teorema 8.6): *Seja* $v : F \to G$ *uma valorização real de* $F$. $F$ *é real fechado se e somente se:*

(a) $G$ *é divisível.*

(b) $F_v$ *é real fechado.*

(c) $(F,v)$ *é henseliano.*

Com os Teoremas 4.2 e 4.3 é fácil obter um exemplo de corpo h.e. que não é real fechado.

Lembramos que um corpo valorizado $(F,v)$ com car $F_v = 0$ é 2-henseliano se não possui extensão algébrica imediata de grau par.

EXEMPLO: Seja $F = R((G))$ o corpo das séries formais com expoentes em $G$ e coeficientes em $R$, onde $G$ é um grupo abeliano, ordenado, não divisível mas 2-divisível e $R$ é um corpo real fechado. Em $F$ temos a valorização $v$ dada por $v(\sum_{g \in G} a_g x^g) = \min\{g \in G;\ a_g \neq 0\}$. O corpo de resíduos de $v$ é isomorfo a $R$ e, portanto, é hereditariamente euclideano. O grupo de valores é $G$ e, portanto, é 2-divisível. O corpo $(F,v)$ é henseliano e, portanto, como car $F_v = 0$, $(F,v)$ é 2-henseliano (Proposição 2.43(b)). Assim, $R((G))$ é hereditariamente euclideano. $R((G))$ não é real fechado pois, $G$ não é divisível.

As proposições 4.4 e 4.5 fornecem exemplos de corpos de números algébricos que são h.e. e que não são reais fechados.

4.4 - PROPOSIÇÃO (Geyer, [PZ] Satz 3.4): *Seja* $\tilde{Q}$ *o fecho algébrico do corpo dos números racionais . Um corpo* $F$ *tal que* $F \subset \tilde{Q}$ *é hereditariamente euclideano se e somente se* $F = R_1 \cap R_2$ *onde* $R_1, R_2 \subset \tilde{Q}$ *são reais fechados e isomorfos sobre sua intersecção.*

4.5 - PROPOSIÇÃO ([PZ] Satz 3.5): *Sejam* $F$ *um corpo* f.r. *e* $\bar{F}$ *um fecho real de* $F$. *Se* $f \in F[x]$ *é um polinômio de grau ímpar, com número de raizes em* $\bar{F}$ *menor que* $(\partial f)^{1/2}$, *então, existe um corpo h.e.* $K$ *tal que* $F \subset K \underset{\neq}{\subset} \bar{F}$.

A importância dos corpos h.e. no estudo das formas quadráticas sobre corpos de funções algébricas torna-se clara no Teorema 4.8. Esse teorema caracteriza os corpos de funções algébricas que satisfazem a L.S.F. e ao mesmo tempo mostra que valem em $F(x)$ princípios de "going up" e "going down". Na sua demonstração serão usados o Lema 4.6 e o Lema 4.7.

4.6 - LEMA: *Sejam* $(F,P)$ *um corpo ordenado e* $(\bar{F},\bar{P})$ *o seu fecho real. Se existe* $\gamma \in \bar{F}$ *tal que* $F(\gamma)$ *possui mais que uma ordem então, o conjunto* $\{\eta : \eta \in \bar{F}$ *e* $F(\eta)$ *possui mais que uma or-*

*dem} é denso em* $(\bar{F},\tau_{\bar{P}})$.

DEMONSTRAÇÃO: Sejam $\alpha \in \bar{F}$, $U(\alpha,\varepsilon) \in \tau_{\bar{P}}$ uma vizinhança arbitrária de $\alpha$ e $\delta \in \bar{P}$ tal que $F(\alpha,\gamma) = F(\delta)$. Seja $\beta \in \{\alpha + \frac{1}{n} \cdot \frac{\varepsilon}{1+\delta}$ com $n \geq 1\}$ e vamos denotar por $\geq$ a relação determinada em $\bar{F}$ por $\bar{P}$. Como $\bar{F}$ é uma extensão algébrica de $F$, dado $a \in \bar{F}$ existe $u \in \bar{P}$ tal que $|a| \leq u$ (por 1.10(iii)). Logo, para todo $a > 0$ existe $b \in P - \{0\}$ tal que $b \leq a$ pois, se $b > a$ para todo $b \in P - \{0\}$ então, $\frac{1}{a} > \frac{1}{b}$ para todo $b \in P - \{0\}$, contrariando a existência de um $u \in P$ tal que $|\frac{1}{a}| \leq u$. Assim, podemos assumir $\varepsilon \in F$ e, portanto, $F \subset F(\beta) \subset F(\delta)$. Desde que há apenas um número finito de corpos intermediários entre $F$ e $F(\delta)$, existem $\beta_i = \alpha + \frac{1}{n_i} \cdot \frac{\varepsilon}{1+\delta}$ e $\beta_j = \alpha + \frac{1}{n_j} \cdot \frac{\varepsilon}{1+\delta}$ com $n_i \neq n_j$ tais que $F(\beta_i) = F(\beta_j)$. Mas então $F(\beta_i) = F(\beta_j) = F(\delta)$, pois $F(\beta_i) = F(\beta_j)$ implica que $\alpha + \frac{1}{n_i} \cdot \frac{\varepsilon}{1+\delta} - (\alpha + \frac{1}{n_j} \cdot \frac{\varepsilon}{1+\delta}) = \frac{(n_j - n_i)\varepsilon}{n_i n_j (1+\delta)} \in F(\beta_i)$ e consequentemente $1 + \delta$ (e, portanto $\delta$) $\in F(\beta_i)$. Assim, $F(\beta_i)$ possui mais que uma ordem pois, pela Proposição 2.38, $F(\delta)$ possui mais que uma ordem. Como $\alpha < \beta_i < \alpha + \varepsilon$, o resultado segue. ∎

No Lema 4.7 vamos considerar valorizações reais de $F(x)$, triviais sobre $F$, que se estendem a extensões finitas formalmente reais de $F(x)$. Da teoria de valorizações e da definição de valorização real sabemos que a cada polinômio irredutível $f \in F[x]$ tal que $\frac{F[x]}{(f)}$ é f.r. corresponde uma valorização real de $F(x)$, trivial sobre $F$. Assim, se $P$ é uma ordem de $F$ e $(\bar{F},\bar{P})$ é o fecho real de $(F,P)$, todo $\alpha \in \bar{F}$ determina uma valorização real de $F(x)$ trivial sobre $F$. Basta considerar o polinômio minimal de $\alpha$ sobre $F$ e observar que o corpo de resíduos da valorização a ele associada é isomorfo a $F(\alpha)$. Denotaremos por $v_\alpha$ tais valorizações de $F(x)$.

4.7 - LEMA: *Sejam* $x$ *um elemento transcendente sobre um corpo* $F$, $(K,P)$ *uma extensão finita ordenada de* $F(x)$ *e* $(\bar{F},\overline{P \cap F})$ *o fecho real de* $(F,P \cap F)$. *Então, existem* $\alpha \in \bar{F}$ *e* $\varepsilon \in \overline{P \cap F}$ *tais que, para todo* $\beta \in U(\alpha,\varepsilon) \in \tau_{\overline{P \cap F}}$ *a valorização* $v_\beta$ *se estende a uma valorização real de* $K$.

DEMONSTRAÇÃO: Sejam $K = F(x)(\rho)$, $f_0 = \frac{h_n}{g_n} y^n + \ldots + \frac{h_0}{g_0} \in F(x)[y]$ tal que $f_0 = Irr(\rho,y,F(x))$ e $m = M.M.C.(g_0,\ldots,g_n)$. Então $f = mf_0 \in F[x,y]$. Podemos supor, por 1.10 (iv) e 1.12, que $(\bar{F},\overline{P \cap F})$ está contido no fecho real $(\bar{K},\bar{P})$ de $(K,P)$. Então, existem $\alpha \in \bar{F}$ e $\varepsilon \in \overline{P \cap F}$ tais que $f(\beta,y)$ possui um único zero simples em $\bar{F}$ para todo $\beta \in U(\alpha,\varepsilon)$ (por [P] Teorema 5.13). Logo, desde que $\bar{F}$ é real fechado e $f(\beta,y) \in \bar{F}[y]$, $f(\beta,y)$ se decompõe em um fator do tipo $y-a$ e fatores do tipo $(y-a)^2 + b^2$ com $a,b \in \bar{F}$. Assim, $f(\beta,y)$ muda de sinal em $\bar{F}$, isto é, existem $\gamma_1$ e $\gamma_2 \in \bar{F}$ tais que $f(\beta,\gamma_1) \cdot f(\beta,\gamma_2) \notin \overline{P \cap F}$

Seja $\bar{v}_\beta : \bar{F}(x) \to \mathbb{Z}$ a valorização real trivial sobre $\bar{F}$ determinada em $\bar{F}(x)$ pelo polinômio $x-\beta$. A restrição de $\bar{v}_\beta$ a $F(x)$ coincide com a valorização $v_\beta$ de $F(x)$. Sejam $P'$

uma ordem de $\bar{F}(x)$ compatível com $\bar{v}_\beta$ (P' existe por 2.25) e $(\overline{\bar{F}(x)},\overline{P'})$ o fecho real de $(\bar{F}(x), P')$. Então, pelo Teorema 2.30, $\bar{v}_\beta$ se estende a uma valorização real $\bar{\bar{v}}_\beta$ de $\overline{\bar{F}(x)}$ e seu corpo de resíduos é $\bar{F}$. Observando que a imagem de $x$ em $\bar{F}$ é $\beta$ e escolhendo $z_1, z_2 \in \overline{\bar{F}(x)}$ tais que suas imagens em $\bar{F}$ sejam respectivamente $\gamma_1$ e $\gamma_2$ temos que $f(x,z_1) \cdot f(x,z_2) \notin \overline{P'}$. Mas então, por 1.10(i), $f(x,y)$ possui um zero em $\overline{\bar{F}(x)}$ e portanto $K$ pode ser imerso em $\overline{\bar{F}(x)}$. O que mostra que $v_\beta$ pode ser estendido a uma valorização real de $K$. ∎

4.8 - TEOREMA: *Sejam* F *um corpo* f.r. *e* x *um elemento transcendente sobre* F. *As seguintes afirmações são equivalentes:*

(1) F *é hereditariamente euclideano.*

(2) F(x) *satisfaz a* L.S.F..

(3) *Para toda extensão algébrica formalmente real de* F(x) *vale a* L.S.F..

(4) *Existe extensão finita formalmente real de* F(x) *que satisfaz a* L.S.F..

DEMONSTRAÇÃO: (1) ⇒ (2) Sejam $v: F(x) \to H$ uma valorização real, $w: F \to G$ a restrição de $v$ a $F$ e $\Delta$ o fecho divisível de $G$ em $H$. Para todo $\gamma \in \Delta$ existe $n \in \mathbb{N}^{*}$ ($n$ mínimo) tal $n\gamma \in G$. Como $F$ é h.e., $n\gamma = 2g$, com $g \in G$. Se $n = 2k$, com $k \in \mathbb{N}$, então $2k\gamma = 2g$ e, como $H$ é livre de torção, $k\gamma = g$, o que contradiz $n$ ser mínimo. Logo, $m = 2k+1$, com $k \in \mathbb{N}$. Assim, $(2k+1)\gamma = 2g$ e, portanto, $\gamma = 2(g - k\gamma) \in 2\Delta$, isto é, $\Delta$ é

2-divisível.

(i) Se $H/G$ é um grupo de torção então $\Delta = H$ e, portanto, $o(H/2H) = 1$.

(ii) Se $H/G$ não é grupo de torção então existe $z \in F(x)$ tal que $v(z) \notin \Delta$. Como $z = \frac{f}{p}$ com $f, p \in F[x]$ e $v(z) = v(f) - v(p)$ temos que $v(f) \notin \Delta$ ou $v(p) \notin \Delta$. Suponhamos que $v(f) \notin \Delta$ e que $\partial f \leq \partial f_i$ para todo $f_i \in F[x]$ tal que $v(f_i) \notin \Delta$. Temos que $f$ é irredutível, $\partial f > 0$ e qualquer que seja $q \in F[x]$,

$$q = \sum_{i=0}^{r} a_i f^i \text{ com } a_i \in F[x], \ \partial a_i < \partial f \text{ e } v(a_k f^k) \neq$$

$\neq v(a_j f^j)$ se $k \neq j$. Pois, como $v(a_i) \in \Delta$ para todos os $a_i$, se $v(a_k f^k) = v(a_j f^j)$ e $k \neq j$ então, $(j-k)v(f) = v(a_k) - v(a_j) \in \Delta$, isto é, $v(f) \in \Delta$. Logo $v(q) = \min_{0 \leq i \leq r} \{v(a_i f^i)\} = \min_{0 \leq i \leq r} \{v(a_i) + iv(f)\}$. Assim $v(q) = \delta_q + i_q v(f)$ com $\delta_q \in \Delta$ e $i_q \in \mathbb{N}$. Seja, agora, $\frac{q}{\ell} \in F(x)$. Como $q \in F[x]$ e $\ell \in F[x]$ temos que $v(\frac{q}{\ell}) = v(q) - v(\ell) = (\delta_q + i_q v(f)) - (\delta_\ell + i_\ell v(f)) =$
$= (\delta_q - \delta_\ell) + (i_q - i_\ell)v(f) \in \Delta \oplus v(f)\mathbb{Z}$. Assim, $H \simeq \Delta \oplus \mathbb{Z}$, $2H \simeq \Delta \oplus 2\mathbb{Z}$ e portanto, $o(H/2H) = 2$. Como $H/G$ não é de torção a dimensão $r(H/G)$ do $\mathbb{Q}$-espaço vetorial $H/G \otimes_{\mathbb{Z}} \mathbb{Q}$ (= ao número máximo de elementos de $H/G$ linearmente independentes sobre $\mathbb{Z}$) é diferente de zero. Logo, desde que

*grau transc.* $F(x)_v \mid F_w + r(H/G) \leq$ *grau transc.* $F(x) \mid F$ (ver [$B_0$] §10, nº3, Corolário 1)

e grau transc. $F(x) \mid F = 1$ temos que $F(x)_v \mid F_w$ é uma extensão algébrica. Assim, como $F_w$ é h.e. (pelo Teorema 4.2) e $v$ é uma valorização real, concluímos que $F(x)_v$ possui uma única ordem.

Portanto, pelo Teorema 2.27, $F(x)$ satisfaz a L.S.F.

(2) ⇒ (1) Sejam $K = F(\alpha)$ uma extensão finita f.r. de $F$ e $f \in F[x]$ o polinômio minimal de $\alpha$ sobre $F$. Então $f$ determina uma valorização real de $F(x)$ com grupo de valores $\mathbb{Z}$ e corpo de resíduos $K$. Como $X_{F(x)} = Y_{F(x)}$, temos, pelo Teorema 2.27, que $|X_K| = 1$. Se $K$ é uma extensão algébrica infinita de $F$ com duas ordens $\leq$ e $\leq_1$, então $F(a)$, com $a \in K$ tal que $a < 0$ e $a >_1 0$, é uma extensão finita de $F$ com duas ordens, o que contraria o que já mostramos. Logo, $F$ e toda extensão algébrica f.r. de $F$ possuem uma única ordem e portanto, $F$ é hereditariamente euclideano.

(1) ⇒ (3) Sejam $v: F(x) \to H$ uma valorização real tal que $o(H/2H) = 2$ e $w: F \to G$ a restrição de $v$ a $F$. Então $r(H/G) \neq 0$, pois $r(G/H) = 0$ implica em $o(H/2H) = 1$, uma vez que, pelo Teorema 4.2., $o(G/2G) = 1$. Logo, grau transc.$(F(x)_v \mid F_w) = 0$ isto é, $F(x)_v \mid F_w$ é uma extensão algébrica. E, portanto, como $v$ é uma valorização real e $F_w$ é h.e. (pelo Teorema 4.2), $F(x)_v$ é h.e.. Pela Proposição 2.33 obtemos, então, que toda extensão algébrica f.r. de $F(x)$ satisfaz a L.S.F..

(3) $\Rightarrow$ (4) Imediata.

(4) $\Rightarrow$ (1) Sejam $K$ a extensão finita f.r. de $F(x)$ que satisfaz L.S.F., $P$ uma ordem de $K$ e $(\bar{F},\overline{P \cap F})$ o fecho real de $(F,P \cap F)$. Pelo Lema 4.7 existem $\alpha \in \bar{F}$ e $\varepsilon \in \overline{P \cap F}$ tais que, para todo $\beta \in U(\alpha,\varepsilon) \in \tau_{\overline{P \cap F}}$, $v_\beta$ se estende a uma valorização real de $K$.

Suponhamos que $\bar{F}$ não é h.e. e seja $\gamma \in \bar{F}$ tal que $F(\gamma)$ possui mais que uma ordem. Então pelo Lema 4.6, existe $\beta_1 \in U_\alpha$ tal que $F(\beta_1)$ possui mais que uma ordem. Consideremos $w$ a extensão de $v_{\beta_1}$ a $K$. O corpo de resíduos $K_w$ de $w$ é uma extensão finita f.r. de $F(\beta_1)$. Portanto, por 2.38, $K_w$ possui mais que uma ordem, e isso, por 2.27, é uma contradição, pois o grupo de valores $G_w$ de $w$ é isomorfo a $\mathbb{Z}$. Logo, $F$ é h.e.∎

Observamos que pelo teorema, o princípio de "going up" vale para toda extensão algébrica de $F(x)$. E o "going down", como era de se esperar, vale para extensões algébricas finitas. Se $K$ é uma extensão infinita de $F(x)$ é possível que $X_K = Y_K$ sem que $X_{F(x)} = Y_{F(x)}$. Basta considerar $K$ como sendo o fecho real relativo a uma ordem $P$ de $F(x)$ e $F$ não hereditariamente euclideano.

É interessante, notar ainda, que se $F$ é um corpo f.r. e $K = F(x_1,\dots,x_n)$ é uma extensão puramente transcendente de $F$, como pelo menos duas indeterminadas independentes, então pode ocorrer $X_K \neq Y_K$ ainda que $F$ seja h.e.. Um exemplo disso, é corpo $\mathbb{R}(x,y)$, conforme mostramos no Capítulo II.

## §2 - PRINCÍPIOS DE NATUREZA LOCAL-GLOBAL EM $F(x)$

Seja $(K,P)$ uma extensão ordenada de um corpo $F$. Lembramos que $F$ é cofinal em $K$ relativamente a $P$ se, para todo $a \in K$ existe $b \in F$ tal que $|a| \leq b$.

4.9 - PROPOSIÇÃO: *Sejam $F$ um corpo h.e., $(K,P)$ uma extensão finita e ordenada de $F(x)$ tal que $F$ não é cofinal em $K$ relativamente a $P$, $v_F$ a valorização real de $K$ associada ao anel $A(F,P)$ e $(\hat{K},\tau_{\hat{v}_F})$ o completamento de $(K,\tau_{v_F})$.*

*Uma forma quadrática $\rho = \langle a_1,\dots,a_n\rangle$ sobre $K$ tal que $v_F(a_i) = 0$, para $i=1,\dots,n$, é indefinida relativamente a $P$ se e somente se $\rho$ é (fracamente) isotrópica em $\hat{K}$.*

DEMONSTRAÇÃO: Observamos que $v_F$ é trivial sobre $F$ pois $F \subset A(F,P) \setminus M(F,P)$. Logo $v_F$ é uma extensão de uma valorização real de $F(x)$ trivial sobre $F$ e, como $[K : F(x)] < \infty$, $K_{v_F}$ é uma extensão finita de $F$. Assim, desde que $F$ é h.e., $K_{v_F}$ possui exatamente uma ordem $\bar{P}$. Para todo $a \in K$ tal que $v_F(a)=0$ temos, então, $a \in P \leftrightarrow [a] \in \bar{P}$. Logo $\rho$ é indefinida relativamente a $P$ se e somente se $\bar{\rho}$ é indefinida em $K_v$ relativamente a $\bar{P}$ e, portanto, se e somente se $\bar{\rho}$ é indefinida em $\hat{K}_{\hat{v}_F}$ relativamente a $\bar{P}$, uma vez que $K_{v_F} = \hat{K}_{\hat{v}_F}$, pois, $(\hat{K},\hat{v}_F)$ é extensão imediata de $(K,v_F)$. Como $K_{v_F}$ possui uma única ordem, $X_{\hat{K}_{\hat{v}_F}} = Y_{\hat{K}_{\hat{v}_F}}$ e portanto, $\bar{\rho}$ é indefinida em $(\hat{K}_{\hat{v}_F}, \bar{P})$ se e somente se $\bar{\rho}$ é fracamente isotrópica em $\hat{K}_{\hat{v}_F}$, e mais precisamente, se e somente se, $\bar{\rho}$ é isotrópica em $\hat{K}_{\hat{v}_F}$ pois $K_{\hat{v}_F}$ é pitagórico, uma vez que é euclideano. Mas, isso ocorre, como $(\hat{K},\hat{v}_F)$ é henseliano, se e somente se, $\rho$ é (fracamente) isotrópica em $\hat{K}$. ■

Com essa proposição obtemos, em 4.11, para extensões finitas de corpos de funções racionais em uma indeterminada, um princípio local-global, relativo à isotropia fraca, análogo ao de Hasse-Minkowski para isotropia. Na sua demonstração será usado o seguinte lema:

4.10 - LEMA: *Sejam* F *um corpo,* x *um elemento transcendente sobre* F, K *uma extensão formalmente real de* F *com* $[K:F(x)] < \infty$ e $\rho = \langle a_1,\dots,a_n\rangle$ *uma forma quadrática sobre* K.

*Se* $\rho$ *é indefinida relativamente a quase todas (isto é, a menos de um número finito) as ordens* P *de* K *relativo as quais* F *não é cofinal em* K, *então* $\rho$ *é localmente isotrópica em* K.

DEMONSTRAÇÃO: Suponhamos que existe uma ordem $P(\leq)$ de K tal que $\rho$ é definida relativamente a P e seja $(\bar{F},\bar{P})$ o fecho real de $(F,P\cap F)$. Podemos supor $0 < a_1,\dots,a_n$. Então P se estende a $K' = K(\sqrt{a_1},\dots,\sqrt{a_n})$. Seja $P = \{n \in \mathbb{N}^{*}$ ; existem n ordens de K com F não cofinal em K e $\rho$ definida em relação a elas $\}$. Pelo Lema 8.7. existe uma valorização real $v_\delta$ de $F(x)$, com $\delta \in \bar{F}$, que se estende a uma valorização real de K'.

Por 2.24 e 2.25 existe uma ordem $P'$ de $K'$ compatível com $v_\gamma$. Como $F$ não é cofinal em $K$ relativamente a $P' \cap K$ e $a_i \in \in P' \cap K$ para todo $1 \leq i \leq n$, pois $a_1, \ldots, a_n$ são quadrados em $K'$, temos que $1 \in P$. Suponhamos que $m \in P$. Então existem ordens $P_1, P_2, \ldots, P_m$ tais que $F$ não é cofinal em $K$ relativamente a $P_i (1 \leq i \leq m)$. A cada $P_i$, com $1 \leq i \leq m$ corresponde uma valorização real $v_{\alpha_i}$ de $K$. Sejam $\gamma_1, \gamma_2, \ldots, \gamma_s$ as raízes dos polinômios irredutíveis correspondentes às valorizações $v_{\alpha_n}, \ldots, v_{\alpha_n}$. Pelo Lema 4.7, podemos escolher $\beta \in \bar{F}$, com $\beta \neq \gamma_i$ para todo $1 \leq i \leq s$, tal que $v_\beta$ se estenda a uma valorização real $v'$ de $K'$. Seja $P'$ a ordem de $K'$ compatível com $v'$. A valorização $v'$ é trivial sobre $F$ e a ordem $P' \cap K$ é diferente de $P_1, \ldots, P_n$, pois $A(F, P' \cap K) \neq \neq A(F, P_i)$. Além disso, $a_1, \ldots, a_n$ são quadrados em $K'$. Logo $m + 1 \in P$. Assim $P = \mathbb{N}^{\cdot}$, o que contraria a hipótese. E, portanto $\rho$ é localmente isotrópica em $K$. ■

4.11 - TEOREMA (Princípio de Hasse-Minkowski relativo a isotropia fraca em $F(x)$): *Sejam* $F$ *um corpo* h.e., $K$ *uma extensão finita, formalmente real de* $F(x)$ *e* $\rho = \langle a_1, \ldots, a_n \rangle$ *uma forma quadrática sobre* $K$.

*Se* $\rho$ *é (fracamente) isotrópica em quase todos os completamentos de* $K$ *relativo a topologias intervalo-aberto induzidas em* $K$ *por ordens em relação as quais* $F$ *não é cofinal em* $K$, *então* $\rho$ *é fracamente isotrópica em* $K$.

DEMONSTRAÇÃO: Como, para todo $1 \leq i \leq n$, $v(F,P)(a_i) \neq 0$ para apenas um número finito de ordens triviais sobre $F$, pela Proposição 4.9, $\rho$ é indefinida em $K$ realtivamente a quase todas as ordens de $K$ triviais sobre $F$. Assim, pelo Lema 4.10, $\rho$ é t.i. em $K$ e, como, pelo Teorema 4.8, $K$ satisfaz a L.S.F., $\rho$ é fracamente isotrópica em $K$. ■

O Teorema 4.5 e o Teorema 4.11 nos levam a analisar, agora, a questão do u-invariante (conforme definido em 1.24) de $F(x)$ (com $F$ h.e.) e de suas extensões finitas que sejam formalmente reais. Com essa finalidade vamos considerar o seguinte princípio: "$H_n$ : Toda forma quadrática localmente isotrópica (= t.i.) de dimensão $n$ é isotrópica."

Lembrando que definimos $u(K) = \text{máx}\{\dim \rho,\ \rho$ é t.i. e anisotrópica em $F\}$, podemos observar que para um corpo $K$ qualquer $u(K) = \min\{n \in \mathbb{N};\ K$ satisfaz $H_m$ para todo $m \geq n+1\}$. Se $K$ não satisfaz $H_n$ para nenhum $n \in \mathbb{N}$ então $u(K) = \infty$.

Para mostrar resultados referentes ao $H_n$ lembramos a definição de formas quadráticas equivalentes: *Duas formas quadráticas* $\rho_1(X_1,\ldots,X_n)$ *e* $\rho_2(X_1,\ldots,X_n)$ *de dimensão* $n$ *sobre um corpo* $F$ *são ditas equivalentes se existe uma matriz inversível* $A$ *do tipo* $n \times n$, *com coeficientes em* $F$ *tal que* $\rho_1(AX) = \rho_2(X)$ *onde* $X$ *denota a transposta da matriz linha* $(X_1,\ldots,X_n)$; isto é, $\rho_2$ é obtida de $\rho_1$ por uma transformação linear não singular das indeterminadas $X_1,\ldots,X_n$. Denotamos por $\rho_1 \sim \rho_2$ essa equivalência.

Alguns resultados elementares relativos a formas quadráticas sobre um corpo $F$ e dos quais faremos uso são:

(i) Se $f \sim g$ então $f$ é isotrópica se e somente $g$ é isotrópica.

(ii) Se $f = \langle a_1,\dots,a_n\rangle$ e $g = \langle b_1,\dots,b_n\rangle$ e $f \sim g$ então $a_1a_2\dots a_n = b_1b_2\dots b_n \dot{F}^2$.

(iii) Se $F$ é f.r. então $f \sim g \Rightarrow A_P(f) = A_P(g)$ para todo $P \in X_F$.

(iv) $\langle a_1,\dots,a_n\rangle$ é isotrópica se e somente se para todo $b \in F^{\bullet}$ a forma $\langle b\rangle \otimes \langle a_1,\dots,a_n\rangle$ é isotrópica.

(v) $\rho = \langle a_1,\dots,a_n\rangle$ e dita hiperbólica se $\rho \sim m\langle 1,-1\rangle$ para algum $m \in \mathbb{N}$.

(vi) Se $x_i \in \dot{F}^2 (1 \le i \le n)$ então as formas $\langle a_1,\dots,a_n\rangle$ e $\langle a_1x_1,\dots,a_nx_n\rangle$ são equivalentes.

(vii) $\rho = \langle a_1,\dots,a_n\rangle$ representa um elemento $b \in F$ se e somente se $\langle a_1,\dots,a_n,-b\rangle$ é isotrópica.

(viii) Se $\langle a_1,\dots,a_n\rangle$ representa $b \in F^{\bullet}$ então existem $a_2',\dots,a_n' \in F$ tais que $\langle a_1,\dots,a_n\rangle \sim \langle b,a_2',\dots,a_n'\rangle$.

Os dois primeiros resultados (4.12 e 4.13) sobre $H_n$ que apresentaremos mostram que se um corpo $F$ satisfaz $H_2$ então $F$ é pitagórico e satisfaz $H_3$.

4.12 - PROPOSIÇÃO: *Seja* $F$ *um corpo.* $F$ *satisfaz* $H_2$ *se e somente se* $F$ *é pitagórico.*

DEMONSTRAÇÃO: Seja $\rho = \langle a_1, a_2 \rangle$, com $a_i \in F$, uma forma quadrática binária sobre $F$ total indefinida. $\rho$ é isotrópica se e somente se $\langle a_1 \rangle \otimes \langle a_1, a_2 \rangle \sim \langle 1, a_1, a_2 \rangle$ é isotrópica. Assim basta considerar as formas do tipo $\langle 1, b \rangle$ com $b$ percorrendo os elementos totalmente negativos de $F$. Logo $-b$ percorre todas as somas de quadrados de elementos de $F$ e como $\langle 1, b \rangle$ é isotrópica se e somente se existem $x_1, x_2 \in F^\bullet$ tais que $x_1^2 = -bx_2^2$ o resultado segue. ∎

A proposição 4.13 estabelece que todo corpo pitagórico satisfaz $H_3$.

4.13 - PROPOSIÇÃO: *Sejam* $F$ *um corpo pitagórico e* $\rho$ *uma forma quadrática sobre* $F$ *de dimensão* $\leq 3$. *Então,* $\rho$ *é isotrópica se e somente* $\rho$ *é localmente isotrópica.*

DEMONSTRAÇÃO: ($\Rightarrow$). É imediato por 1.30.

($\Leftarrow$) Seja $\rho = \langle a_1, a_2 \rangle$ com $a_1 a_2 \notin P$, qualquer que seja $P \in X_F$. Então, $-a_1 a_2 \in \bigcap_{P \in X_F} P = \Sigma F^2 = F^2$ e, assim, $a_1 a_2 = -t^2$, isto é, $a_2 = -a_1 (\frac{t}{a_1})^2$ com $t \in F$. Logo, $\langle a_1, a_2 \rangle = \langle a_1, -a_1 (\frac{t}{a_1})^2 \rangle \sim \langle a_1, -a_1 \rangle$ e, portanto $\rho$ é isotrópica.

Como $\langle a,b,c \rangle$ é isotrópica se e somente se $abc \langle a,b,c \rangle \sim \langle bc, ac, ab \rangle \sim \langle ab, bc, ab, bc \rangle$ é isotrópica, basta considerar as formas ternárias do tipo $\langle a, b, ab \rangle$. Seja, pois, $\rho = \langle a, b, ab \rangle$ uma forma sobre $F$, localmente isotrópica. Então, $\langle 1, a, b, ab \rangle$ é localmente isotrópica e, portanto hiperbólica nos fechos reais $F_P$ de $(F,P)$ para todo $P \in X_F$ ( [L] , Capítulo X , Corolário 1.9). Assim, pelo Princípio Local Global de Pfister para corpos pitagóricos ( [L] Capítulo VII, Teorema 4.1), $<1,a,b,ab> \sim <1,-1,1,-1>$ em F. Como $<1> \oplus <a,b,ab> \sim <1,a,b,ab> \sim <1,-1,1,-1> \sim <1> \oplus <-1,1,1>$, pelo Teorema de cancelamento de witt ( [L] Capítulo I, Teorema 4.2), temos que $<a,b,ab> \sim <-1,1,-1>$ em F. E, portanto, $\rho$ é isotrópica em F. ∎

A proposição 4.14, além de fornecer um resultado interessante por si só, será usado na demonstração da Proposição 4.16, a qual por sua vez será útil na demonstração do Teorema 4.17 onde mostramos que se F é h.e., então, $u(K) \leq 2$, para toda extensão finita f.r. de $F(x)$.

4.14 - PROPOSIÇÃO: *Seja* $n$ *um número natural fixo tal que* $n \geq 4$. *Se* F *satisfaz* $H_n$ *então* $X_F = Y_F$.

DEMONSTRAÇÃO: Seja $\rho = <-1,a,b,ab>$ uma forma quadrática sobre F e $\rho_1 = <a,b,ab> \oplus (n-3)<-1>$. Como $\rho_1$ é t.i. e F satisfaz $H_n$, $\rho_1$ é isotrópica em F. Logo $(n-3)\rho$ é isotrópica em F e, portanto, $\rho$ é fracamente isotrópica. Assim, toda forma do tipo $<1,a,b,-ab>$ é fracamente isotrópica e, pelo Teorema 1.32, $X_F = Y_F$. ∎

Assumindo que F é pitagórico temos pelo Corolário 1.33, a seguinte recíproca forte da Proposição 4.14: *Se* $X_F = Y_F$ *então* F *satisfaz* $H_n$ *para todo* $n \geq 2$. Porém, se F não é pi tagórico a recíproca em geral é falsa.

4-15 - EXEMPLO: Seja $K = F((x))$ onde $F$ é f.r. O corpo $(F((x)),v)$, onde $v$ é definida por $v(\sum_{i=m}^{\infty} a_i x^i) = m$ se $a_m \neq 0$, é um corpo henseliano com corpo de resíduos $F$ e grupo de valores $\mathbb{Z}$. Logo, pelo Teorema 2.45, $X_K = Y_K$ se e somente se $F$ possui uma única ordem. Suponhamos que $F$ possui uma única ordem. Então, $K$ satisfaz algum $H_n$ para $n \geq 2$ se e somente se $F$ é euclideano. De fato: Se $F$ é euclideano, então $F$ é pitagórico e como $X_K = Y_K$, $F$ satisfaz $H_n$ para todo $n \geq 2$. Assumamos, agora, que $K$ satisfaz $H_n$ para algum $n \geq 2$ fixo e suponhamos que $F$ não é euclideano. Então, como $F$ possui uma única ordem, $F$ não é pitagórico. Seja $w \in \Sigma F^2$ tal que $w \notin F^2$. Consideremos a forma $\rho = (n-2)\langle 1\rangle \oplus \langle x\rangle \langle 1,-w\rangle$ sobre $K$. Como $v(x) = 1$ e as formas $(n-2)\langle 1\rangle$ e $\langle 1-w\rangle$ são anisotrópicas em $F$, $\rho$ é anisotrópica em $K$([ L ] Capítulo VI - Corolário 1.9). Como $\dim \rho = n$ e $\rho$ é t.i. chegamos a uma contradição e portanto $F$ é euclideano. Se escolhermos $F = Q$ e $K = Q((x))$, temos que $X_K = Y_K$ mas, $K$ não satisfaz $H_n$ para nenhum $n \geq 2$, pois $Q$ não é euclideano.

4.16 - PROPOSIÇÃO: $H_2 \Rightarrow H_3 \not\Rightarrow H_4 \Rightarrow H_5 \Rightarrow \ldots$

DEMONSTRAÇÃO: Pela Proposição 4.12, se $F$ satisfaz $H_2$ então $F$ é pitagórico e assim pela Proposição 4.13, $F$ satisfaz $H_3$. Logo $H_2 \Rightarrow H_3$.

Seja agora $n \in \mathbb{N}$ com $n \geq 4$ vamos provar que $H_n \Rightarrow H_{n+1}$. Seja $\rho = \langle a_1,\dots,a_{n+1}\rangle$ uma forma quadrática totalmente indefinida. Desde que, pela Proposição 4.14, $X_F = Y_F$, $\rho$ é fracamente isotrópica. Portanto, existe uma equação $\sum_{i=1}^{n+1} a_i w_i = 0$ onde $w_i \in \Sigma F^2$ e $w_i \neq 0$ para algum $1 \leq i \leq n+1$. Podemos assumir que $w_1 = 1$. Suponhamos que $a_1 + w_2 a_2 = 0$. Como $a_1 + w_2 a_2 = 0$ implica em $a_1 . a_2 \in -P$ para todo $P \in X_F$, a forma $\langle a_1,\dots,a_n\rangle$ é t.i. e, portanto, isotrópica. Assim $\rho$ é isotrópica e $H_n \Rightarrow H_{n+1}$. Suponhamos, agora, que $a_1 + w_2 a_2 \neq 0$. A forma $\langle a_1 + w_2 a_2, a_3,\dots,a_{n+1}\rangle$ é t.i. e portanto, como sua dimensão é $n$, ela é isotrópica. Então a forma $\langle a_3,\dots,a_{n+1}\rangle$ representa o elemento $-a_1 - w_2 a_2$ e $\langle a_3,\dots,a_{n+1}\rangle \sim \langle -a_1, -w_2 a_2, a_4',\dots,a_{n+1}'\rangle$ com $a_i' \in \dot{F}$ para todo $4 \leq i \leq n+1$. Assim, $\langle a_1, a_2,\dots,a_n\rangle \sim$ $\sim \langle a_1, a_2, -a_1 - w_2 a_2, a_4',\dots,a_n'\rangle$. Como essa última forma é t.i., a forma n-dimensional $\langle a_1, a_2,\dots,a_n\rangle$ é t.i. e, portanto, por ser válido $H_n$, ela é isotrópica. Como $\rho$ contém uma sub-forma n-dimensional isotrópica $\rho$ é isotrópica. E assim $H_n \Rightarrow H_{n+1}$.

Para observar que $H_3 \not\Rightarrow H_4$, consideremos o corpo f.r. $F = \mathbb{R}((t_1))((t_2))$. Desde que $F$ é pitagórico, $F$ satisfaz $H_2$ e $H_3$. Como $X_F \neq Y_F$ (Exemplo 2.54) $F$ não satisfaz $H_n$, qualquer que seja $n \geq 4$. As formas $\langle 1, t_1, t_2, -t_1 t_2\rangle$ e $\langle n-3\rangle\langle 1\rangle \oplus \oplus \langle t_1, t_2 - t_1 t_2\rangle$ (para todo $n > 4$), por exemplo, são t.i. e anisotrópicas em $F$.

4.17 - TEOREMA: *Seja* $K$ *uma extensão* f.r. *de* $F(x)$ *com*

$[K : F(x)] < \infty$. *As seguintes afirmações são equivalentes:*

(1) $F$ *é hereditariamente euclideano.*

(2) $X_K = Y_K$

(3) $K$ *satisfaz* $H_n$ *para todo* $n \geq 3$.

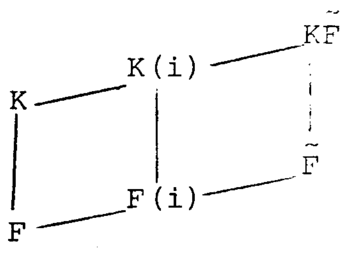
(4) *Toda forma quadrática* $\rho = <a_1, \ldots, a_n>$ *com* $n \geq 3$ *indefinida em quase todas as ordens de* $K$ *relativamente às quais* $F$ *não é cofinal em* $K$, *é isotrópica em* $K$.

DEMONSTRAÇÃO: (1) $\Leftrightarrow$ (2) É imediato, pelo Teorema 4.5 e o Teorema 1.32.

(3) $\Leftrightarrow$ (4) É imediato, pelo Lema 4.10.

(3) $\Rightarrow$ (1) É imediato, pelo Teorema 4.5.

(1) $\Rightarrow$ (3) Sejam $F(i)$, $K(i)$ onde $i^2 = -1$ e $\tilde{F}$ o fecho algébrico de $F(i)$.




Como $F$ é h.e. obtemos, pelo Teorema 4.1 (2), que $[\tilde{F} : F(i)]$ é um número super-natural ímpar. Substituindo $F(i)$ por $F(i) \cap K(i)$ se necessário, podemos assumir $F(i)$ algebri camente fechado em $K(i)$. Assim, como car $F(i) = 0$, $K(i)$ e $\tilde{F}$ são linearmente disjuntos sobre $F(i)$. Logo, $[K\tilde{F} : \tilde{F}]$ é ímpar. Desde que $K\tilde{F}$ é um corpo de funções algébricas em uma variável sobre um corpo algebricamente fechado temos, pelo Teorema 1.22, que $u(K\tilde{F}) \leq 2$. E, pelo Teorema 1.23, concluímos que $u(K(i)) \leq 2$. Mas então, toda forma quadrática $\rho$ sobre $K$ tal que $\dim \rho \geq 3$ e $m\rho$ é hiperbólica para algum $m$ é isotrópica em $K$ (por [EL] (1973) Teorema 4.11(2) se $\rho$ é um elemento de torção no anel de witt e $\dim \rho \leq 3$ então $\rho$ é isotrópica.).

Seja $\rho = \langle a,b,c\rangle$ uma forma quadrática ternária sobre $K$ totalmente indefinida. Então $\rho_0 = \langle a,b,abc\rangle \sim \langle a\rangle \otimes \otimes \langle 1,ab,ac,a^2bc\rangle$ é totalmente indefinida. Mas então, $\rho_0' = \langle 1,ab,ac,a^2bc\rangle$ é t.i. e portanto $A_P(\rho_0') = 0$, qualquer que seja $P \in X_K$. Logo $2^n\rho_0'$ é hiperbólica para algum $n \in \mathbb{N}$ (ver [ P ] (1975) Teorema 10.15) e portanto $\rho_0'$ é isotrópica. Como $\rho_0' = \langle 1,ab\rangle \otimes \langle 1,ac\rangle$ temos que $\rho_0' \sim \langle 1,-1,1,-1\rangle$ (ver [L] Capítulo X, Corolário 1.9). Assim, $\rho_0 \sim \langle a\rangle \otimes \langle 1,-1,1,-1\rangle$ e pelo Teorema de Cancelamento de Witt, $\rho \sim \langle a\rangle \otimes \langle 1,-1,1\rangle$ ou $\rho \sim \langle a\rangle \otimes \langle 1,-1,-1\rangle$. Assim, concluímos que $\rho$ é isotrópica, isto é, $K$ satisfaz $H_3$.

Seja $\rho$ uma forma quadrática sobre $K$ tal que $\rho$ é t.i. e $\dim \rho = 4$. Podemos assumir $\rho = \langle 1,a,b,c\rangle$. Como $X_K = Y_K$ existe $c \in \dot{F}$ tal que $2^n(\langle 1,a\rangle \otimes \langle 1,b\rangle) \sim 2^n(\langle 1,1\rangle \otimes \langle 1,c\rangle)$ para algum $n \in \mathbb{N}$ (por [ P ] (1975) Teorema 9.1 e [EL] (1972) Teorema 3.5(4)). Então, $A_P(\langle 1,a\rangle \otimes \langle 1,a\rangle) = A_P(\langle 1,1\rangle \otimes \langle 1,c\rangle)$ para todo $P \in Y_K$. Assim as formas $\beta_1 = \langle 1,-ab,c\rangle$ e $\beta_2 = \langle a,b,c\rangle$

são t.i. e portanto $\beta_1 \sim \langle 1,-1,x_1\rangle$ e $\beta_2 \sim \langle 1,-1,x_2\rangle$ com $x_1,x_2 \in K$. Como $\langle 1,a,b,-ab\rangle \oplus \langle 1,-1\rangle \sim \langle 1,a,b,-ab\rangle \oplus \langle c,-c\rangle \sim$ $\sim \langle 1,-ab,c\rangle \oplus \langle a,b,c\rangle \sim \langle 1,-1,x_1\rangle \oplus \langle 1,-1,x_2\rangle = 2\langle 1,-1\rangle \oplus \langle x_1,x_2\rangle$, concluímos, pelo Teorema de Cancelamento de Witt, que $\langle 1,a,b,-ab\rangle \sim$ $\sim \langle 1,-1\rangle \oplus \langle x_1,x_2\rangle$. Logo, $\langle 1,a,b,-ab\rangle$ é isotrópica e a forma $\langle 1,a,b\rangle$ representa $ab$ em $K$. Assim, como $\langle 1,a,b\rangle \sim \langle ab,x,y\rangle$ com $x,y \in \dot{F}$ e $xy \in \dot{F}^2$, $\langle 1,a,b,c\rangle \sim \langle ab,x,y,c\rangle \sim \langle ab,x,x,c\rangle$. Mas então, $\langle ab,x,c\rangle$ é t.i. e, pelo que já mostramos isotrópica. Consequentemente $\langle ab,x,y,c\rangle$ e, portanto, $\langle 1,a,b,c\rangle$ é isotrópica. Logo, $K$ satisfaz $H_4$ e, pela Proposição 4.16, $H_n$ para todo $n \geq 4$. ▫

BIBLIOGRAFIA


[ B ] BECKER,E.. "Euklidische Körper und euklidische Hüllen von Körpern". *J.reine angewandte Mathematik*, 268/269 (1974) 41-42.

__________. "Local Global Theorems for diagonal forms of higher degree". *J.reine angewandte Mathematik*, 318 (1980) 36-50.

[Bo] BOURBAKI,N.. *Elements de Mathématique-Algèbre Comutative*, chapitre 6.Hermann, Paris, 1964.

[BR] BRÖCKER,L.. "Zur Theorie der quadratischen Formen über formal reellen Körpern". *Math. Annalen* 210 (1974) 233-256.

[ E ] ENDLER,O.. *Valuation Theory*. Springer Verlag, Berlin-Heidelberg-New York, 1972.

[EL] ELMAN,R., LAM,T.Y.. "Quadratic forms over formally real fields and pythagorean fields". *Amer. J. Math.* 94 (1972) 1155-1194.

________________. "Quadratic forms and the u-invariant I". *Math. Z.* 131 (1973) 283-304.

[ELP] ELMAN,R., LAM,T.Y., PRESTEL,A.. "On some Hasse principles over formally real fields". *Math. Z.* 134 (1973) 291-301.

[ J ] JACOBSON,N.. *Lectures in Abstract Algebra* Vol III. Princeton, von Nostrand, 1966.

[ L ] LAM,T.Y.. *The Algebraic Theory of Quadratic Forms*. W.A.

Benjamin, Reading, Massachussets, 1973.

[ La ] LANG, S.: "The theory of real places". *Annals of Math.* 57 (1953) 378-391.

[ P ] PRESTEL, A. "Quadratische semi-ordnungen und quadratische Formen". *Math. Z.* 133 (1973) 319-342.

_________. "A Local Global principle for quadratic forms". *Math. Z.* 142 (1975) 91-95.

_________. *Lectures on Formally Real Fields*. IMPA, Rio de Janeiro, 1975.

[ PZ ] PRESTEL, A. und ZIEGLER, M.. "Erblich euklidische Körper". *J. reine angewandte mathematik* 274/275 (1975) 196-205.

[ R ] RIBEMBOIN, P.. *L'Aritmetique des corps*. Hermann, Paris, 1972.